KEMI-TORNION AMMATTIKORKEAKOULU

Suunnitelma vesiprosessin etäohjauksen toteuttamiseksi

Ville Tilus

Sähkötekniikan opinnäytetyö
Automaatio
Insinööri(AMK)

KEMI 2012

ALKUSANAT

Haluan kiittää Kemi-Tornion ammattikorkeakoulua opinnäytetyöstä sekä DI Tuomas Pussilaa opinnäytetyön ohjaamisesta. Lisäksi haluan kiittää kaikkia henkilöitä, jotka ovat olleet osallisena työn etenemisessä.

TIIVISTELMÄ

Kemi-Tornion ammattikorkeakoulu, Tekniikan ala	
Koulutusohjelma	Sähkötekniikka
Opinnäytetyön tekijä	Ville Tilus
Opinnäytetyön nimi	Suunnitelma vesiprosessin etäohjauksen toteuttamiseksi
Työn laji	Opinnäytetyö
päiväys	12.4.2012
sivumäärä	44 + 2 liitesivua
Opinnäytetyön ohjaaja	DI Tuomas Pussila
Yritys	Kemi-Tornion ammattikorkeakoulu
Yrityksen yhteyshenkilö/valvoja	DI Tuomas Pussila

Tämä opinnäytetyö tehtiin Kemi-Tornion ammattikorkeakoululle, jonka tekniikan yksikön laboratorioita uudistetaan. Laboratorioiden uudistamiseen kuuluu myös automaatiolaboratorion vesiprosessin etäohjausmahdollisuuden hankinta opetuskäyttöön. Tässä opinnäytetyössä selvitetään vesiprosessin etäohjausmahdollisuudet Siemensin ratkaisuilla. Työn tarkoituksena on kehittää Kemi-Tornion ammattikorkeakoulun aikuisopetusta. Työn tavoitteena oli löytää ratkaisu etäohjaukseen ja toteuttaa se mahdollisuuksien mukaan. Lisäksi tavoitteena oli myös tietoturvan varmistaminen.

Työssä selvitettiin jo käytössä olevat ohjelmistot ja laitteet sekä myös tarvittavat ohjelmistot, ohjelmistopäivitykset ja laitteet etäohjauksen toteuttamiseksi. Lisäksi selvitettiin tarvittava tietoturva. Työssä selvitettiin eri vaihtoehdot etäohjauksen toteuttamiseksi ja valittiin niistä sopivin ratkaisu vesiprosessin etäohjaukseen.

Tämän opinnäytetyön tavoitteet toteutuivat siten, että Siemensiltä löytyi ratkaisu vesiprosessin etäohjaamiseksi. Etäohjausta ei kuitenkaan ainakaan toistaiseksi toteuteta tämän opinnäytetyön pohjalta. Etäohjaus Siemensin ratkaisuilla on kuitenkin mahdollista toteuttaa myös tulevaisuudessa tämän opinnäytetyön pohjalta. Opinnäytetyölle asetetut tavoitteet saavutettiin sovitussa aikataulussa. Työn tuloksena on luotu hankintaesitys sekä suunnitelma valitun etäohjausratkaisun käyttöönottamiseksi. Lisäksi on esitetty etäohjausmahdollisuus käyttäen iLinc-sovellusta.

Asiasanat: prosessinohjaus, tietoturva, käyttöönotto.

ABSTRACT

Kemi-Tornio University of Applied Sciences, Technology

Degree Programme	Electrical Engineering
Name	Ville Tilus
Title	Remote Control of Water Process
Type of Study	Bachelor's Thesis
Date	12 April 2012
Pages	44+ 2 appendixes
Instructor	Tuomas Pussila, MSc, Process Engineering
Company	Kemi-Tornio University of Applied Sciences
ContactPerson/Supervisor from Company	Tuomas Pussila, MSc, Process Engineering

This Bachelor's Thesis was carried out for Kemi-Tornio University of Applied Sciences of which laboratory facilities are being renewed. The purpose of the thesis was to find a solution to remote control a water process located in the laboratory using Siemens software. The main goal was to find a solution and implement it if possible. Remote control of the water process would be useful especially in adult education. The work included also security which is important from the point of view of usability of the water process.

The work begun by getting familiar with the Siemens software to remote control the water process. The work was carried out by listing the current Siemens software used in Kemi-Tornio University of Applied Sciences and finding out the required Siemens software, software updates and device to remote control the water process. The work was carried out by using literature, internet sources and by interviewing experts via e-mail.

The most goals set for this work were reached, but the implementation of the chosen solution was not carried out. The remote control of the water process can be implemented in the future based on this thesis. The contents of this work were also reached on time. As a result of this thesis, a presentation for acquisition for the required software and device was produced. In addition, a deployment plan for the chosen solution was also made.

Keywords: process control, security, deployment.

SISÄLLYSLUETTELO

1. JOHDANTO

Tämä opinnäytetyö liittyy hankkeeseen, jossa Kemi-Tornion ammattikorkeakoulun tekniikan yksikön laboratoriotiloja uudistetaan. Työn lähtökohtana on tarkoitus löytää Kemi-Tornion ammattikorkeakoulun automaatiolaboratoriossa sijaitsevalle vesiprosessille etäohjausratkaisu käyttäen Siemensin ohjelmistoja. Työn tarkoituksena on aikuisopetuksen kehittäminen. Aikuisopetuksen käytössä olevat kontaktitunnit ovat rajalliset, joten vesiprosessin etäohjaus mahdollistaisi aikuisopiskelijoiden etäopetuksen.

Työn tavoitteena on selvittää mahdollisuudet toteuttaa Kemi-Tornion ammattikorkeakoulun automaatiolaboratoriossa sijaitsevan vesiprosessin etäohjaus käyttäen Siemensin ohjelmistoja. Tavoitteena on löytää ratkaisu ja toteuttaa se mahdollisuuksien mukaan. Tarkoituksena on myös selvittää tarvittavat tietoturvaratkaisut.

Työ rajattiin koskemaan ainoastaan Siemensin ohjelmistoja. Työssä luodaan suunnitelma etäohjauksen toteuttamiseksi. Mikäli suunnitelmaa ei toteuteta, jää työ pelkäksi suunnitelmaksi, joka on mahdollista toteuttaa tulevaisuudessa. Työn toteutus on sidottu myös Kemi-Tornion ammattikorkeakoululla käytössä oleviin tietoturvaratkaisuihin

Työssä selvitetään Kemi-Tornion ammattikorkeakoululla jo käytössä olevat Siemensin ohjelmistoversiot sekä selvitetään tarvittavat ohjelmistot ja laitteet etäohjauksen toteuttamiseksi. Lisäksi selvitetään tarvittavat tietoturvaratkaisut vesiprosessin toiminnan varmistamiseksi.

Työ aloitetaan tutustumalla etäohjauksen kohteena olevaan vesiprosessiin, Siemensin ohjelmistoihin, tietoturva-asioihin sekä Siemensin etäohjausratkaisuihin. Työssä esitetään mahdolliset toteutusratkaisut etäohjaukselle sisältäen hankintaesityksen ja käyttöönottosuunnitelman.

2. KEMI-TORNION AMMATTIKORKEAKOULU

Kemi-Tornion ammattikorkeakoulu on toiminut vuodesta 1992. Sillä on yhteensä viisi opetuspistettä Kemissä ja Torniossa, joihin kuuluu myös 4 tieto- ja kirjastopalveluyksikköä. Opiskelijoita Kemi-Tornion ammattikorkeakoulussa on noin 3000 sekä se työllistää noin 250 henkilöä. Korkeakouluopetuksen lisäksi Kemi-Tornion ammattikorkeakoulu tekee tutkimus- ja kehitystyötä alueen hyvinvoinnin ja opetuksen edistämiseksi. Kemi-Tornion ammattikorkeakoulu on yhdessä Lapin Yliopiston ja Rovaniemen ammattikorkeakoulun kanssa osa Lapin korkeakoulukonsernia. Kemi-Tornion ammattikorkeakoulun tekniikan yksikkö sijaitsee Kemissä Kivikon kaupunginosassa. /3/

2.1. Vesiprosessi

Kemi-Tornion ammattikorkeakoulun ulkopuolisen ohjauksen kohteena oleva vesiprosessi (kuvassa 1) sijaitsee Kemi-Tornion ammattikorkeakoulun tekniikan yksikön automaatiolaboratoriossa. Lisäksi laboratorioon kuuluu erillinen valvomohuone, jossa sijaitsevat prosessiasemat sekä ohjelmoitavat logiikat. Vesiprosessi on opetuskäytössä. /7/

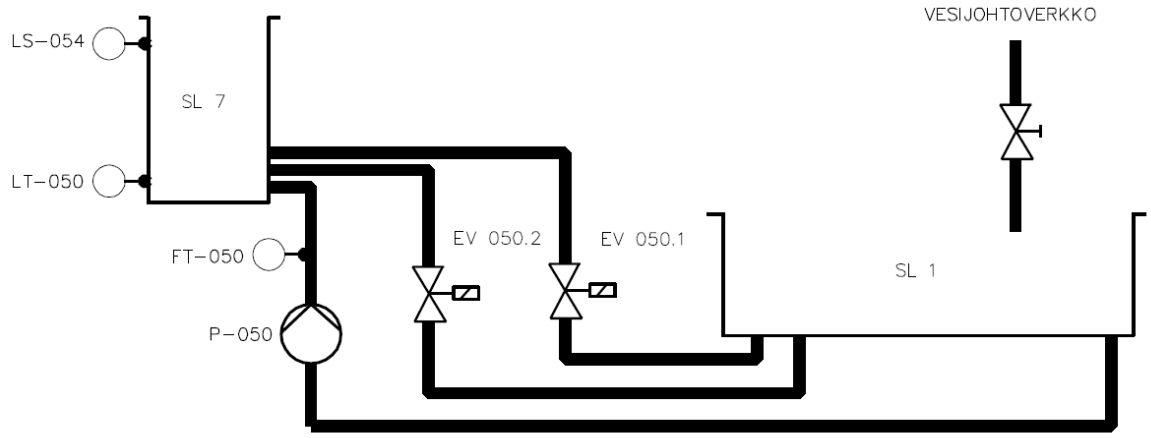
Vesiprosessi sisältää 7 eri säiliötä. Lisäksi prosessiin kuuluu lukuisia kenttälaitteita, öljykattila, lämmönvaihdin prosessiaineena olevan veden lämmitystä varten sekä useita eri pumppuja ja putkistoja. Koko prosessista voidaan erottaa kolme toimintansa puolesta itsenäistä osaprosessia. /7/

Kuva 1. Vesiprosessi /4/

2.1.1. Osaprosessi 1

Osaprosessi 1 (kuvassa 2) käsittää säiliöt SL 7 ja SL 1. SL 1 on varastosäiliö, johon voi käsiventtiilin avulla lisätä vettä suoraan vesijohtoverkosta. Säiliöstä SL 1 voidaan siirtää vettä säiliöön SL 7 taajuusmuuttajalla ohjatun pumpun P-50 avulla. Osaprosessissa on lisäksi 2 paluuvesiputkea, joiden kautta prosessiaine voidaan palauttaa säiliöön SL 1 ohjaamalla magneettiventtiileitä EV 050.1 ja EV 050.2. /7/

Säiliön SL 7 ja pumpun P-50 väliin on asennettu kuristuslaipallinen paine-eroon perustuva virtausmittari ja lähetin, joka mittaa kuristuslaipan molemmille puolille syntyvää paine-eroa ja muuttaa sen eroon verrattavissa olevaksi virtausarvoksi. Virtausmittarin lähetin lähettää virtaustiedon logiikalle virtaviestinä. Säiliössä SL 7 sijaitseva pinnankorkeuslähetin LT-50 mittaa säiliön pinnankorkeuden hydrostaattisesta paineesta ja lähetin lähettää tiedon virtaviestinä logiikalle. Kapasitiivinen anturi LS-054 antaa säiliössä olevan prosessiaineen pinnankorkeustiedon. /7/

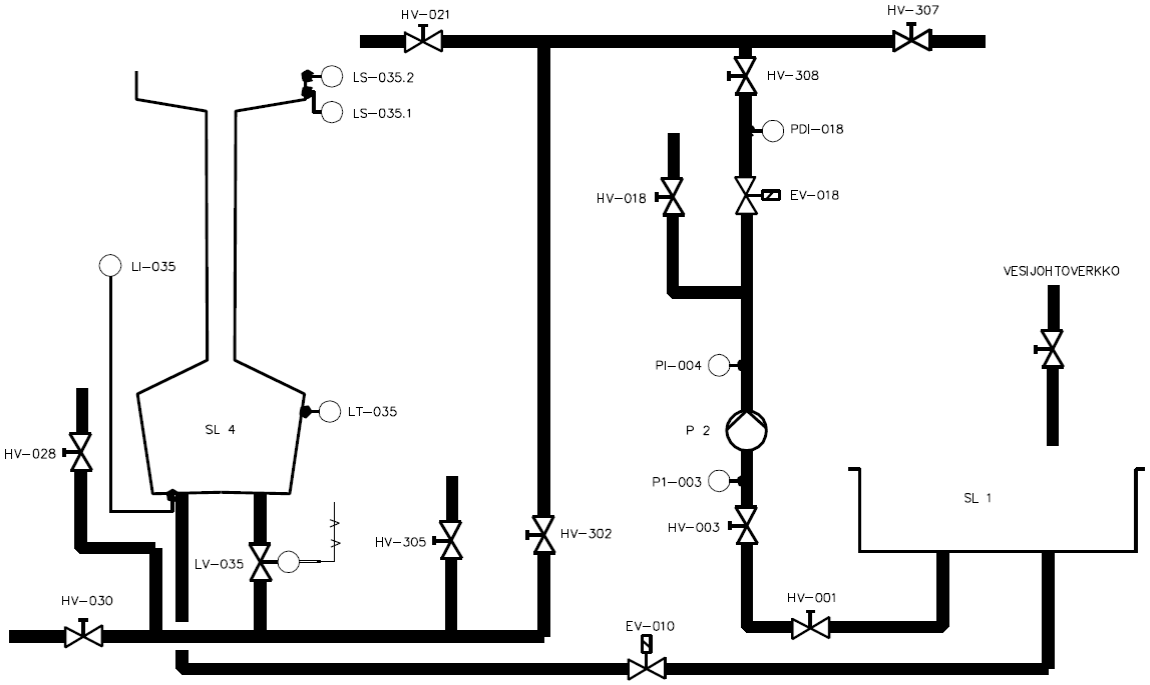


Kuva 2. PI-kaavio osaprosessista 1 /7/

2.1.2. Osaprosessi 2

Osaprosessiin 2 (kuvassa 3) kuuluvat säiliöt SL 4 sekä SL 1, joka on tässäkin osaprosessissa varastosäiliö, johon voi lisätä vettä vesijohtoverkosta. Osaprosessi 2 saadaan toimimaan itsenäisesti sulkemalla käsiventtiilit HV-307, HV-021, HV-305, HV-028, HV-018 sekä HV-030. Käsiventtiilit HV-001, HV-003, HV-308 ja HV-302 tulee olla auki-asennossa, jolloin pumpulla P 2 voidaan pumpata vettä säiliöön SL 4. Pumpun molemmille puolille on asennettu painemittarit (PI-003 ja PI-004), joiden avulla saadaan selville virtauspaine. Virtauspaineen osoittaa myös PDI-018. /7/

Säiliöstä SL 1 voidaan ohjata prosessiainetta säiliöön SL 4 avaamalla magneettiventtiili EV-018 tai säätöventtiili LV-035. Prosessiaineen ohjaus tapahtuu taajuusmuuttajalla ohjatulla pumpulla P 2. Säiliössä SL 4 on pinnanosoitin LI-035, pinnankorkeuden lähetin LT-035 ja kapasitiiviset raja-anturit LS-035.2 ja LS-035.1, joilla mitataan säiliön ylä- ja alarajaa. /7/

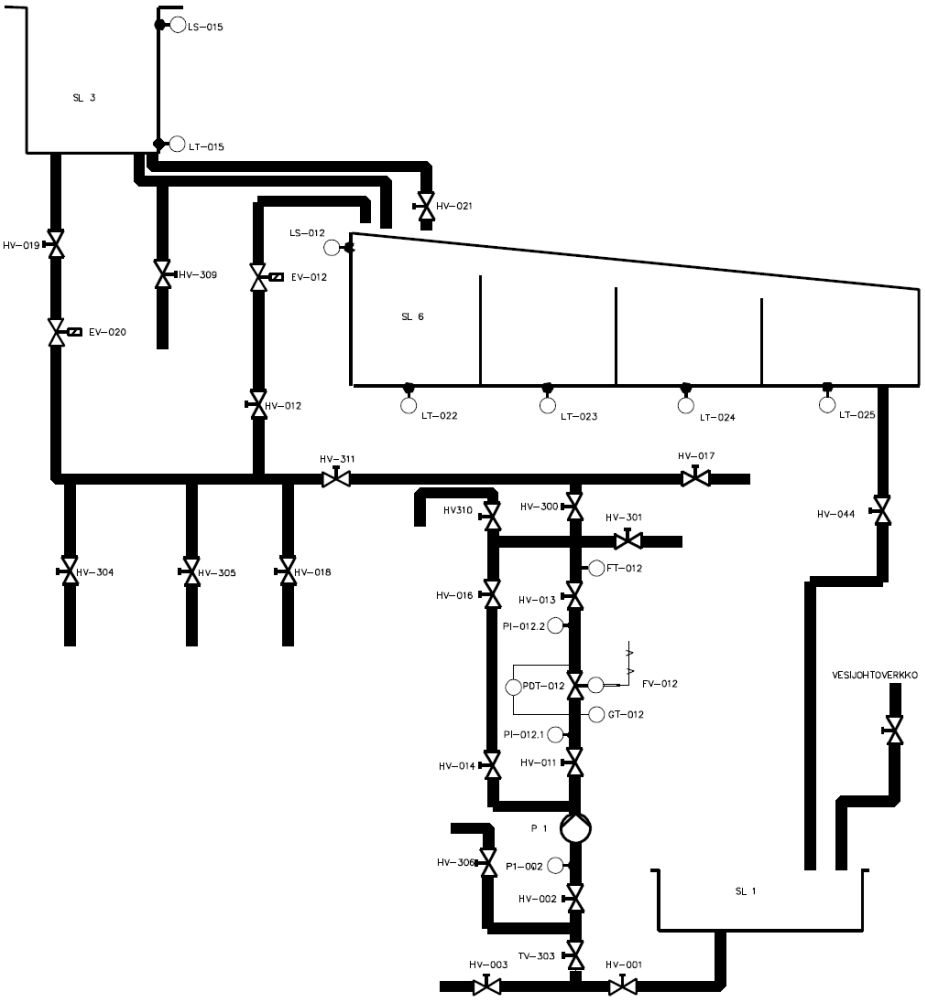


Kuva 3. PI-kaavio osaprosessista 2 /7/

2.1.3. Osaprosessi 3

Kuvassa 4 oleva osaprosessi 3 on selkeästi monimutkaisin näistä kolmesta osaprosessista. Tässäkin osaprosessissa varastosäiliönä toimii SL 1. Osaprosessiin kuuluvat myös säiliöt SL 6 ja SL 3. Osaprosessi voidaan erottaa itsenäisesti toimivaksi käsiventtiileillä HV-003, HV-017, HV-018, HV-021, HV-301, HV-304, HV-305, HV-306, HV-309 ja HV-310. Veden virtaus sallitaan avaamalla käsiventtiilit HV-001, HV-002, HV-011, HV-012, HV-013, HV-019, HV-044, HV-300, HV-301 ja TV-002. Säätöventtiili FV-012 voidaan myös tarvittaessa ohittaa käyttäen apuna käsiventtiileitä HV-014 ja HV-016. /7/

Säiliössä SL 3 sijaitsee pinnankorkeuden lähetin LT-015 sekä pinnankorkeuden ylärajaa mittaava kapasitiivinen anturi LS-015. Säiliön SL 6 jokaiselle neljälle eri lohkolle on oma pinnankorkeudenlähetin (LT-022, LT-023, LT-024 ja LT-25). Lisäksi säiliössä SL 6 sijaitsee pinnankorkeusanturi LS-012. Pumppua P 1 ohjataan taajuusmuuttajalla analogisen virtaviestin avulla. Pumpun P 1 lähellä sijaitsee paine-eromittari PDT-012 ja asentolähetin GT-012. /7/



Kuva 4. PI-kaavio osaprosessista 3 /7/

2.2. Kemi-Tornion ammattikorkeakoulun tietoverkko

Kemi-Tornion ammattikorkeakoulun sisäverkossa on käytössä omat verkkotunnukset opiskelijoille, henkilökunnalle sekä vierailijoille. Vierailijoiden tunnuksia voi käyttää ainoastaan lyhytaikaisilla käyttäjätunnuksilla ilman erillistä käyttöoikeussopimusta. Verkkoa voivat käyttää kaikki, joiden käyttäjätunnukset ovat voimassa Kemi-Tornion ammattikorkeakoulun verkossa. Näin estetään ulkopuolisten pääsy tietoverkkoon sekä voidaan jaotella tietoverkkoa eri käyttötarkoituksia varten. Kemi-Tornion ammattikorkeakoululla on käytössä langaton verkko (WLAN). Verkko kuuluu

tärkeimmissä yleisissä tiloissa, auditorioissa, neuvotteluhuoneissa ja laboratorioissa. Langattomassa lähiverkossa on käytössä 802.1X-standardin mukainen www-pohjainen autentikointi. Lisäksi käytössä on sisäinen intranet sekä muun muassa iLinc-ohjelmisto, jolla voidaan toteuttaa etäopetusta. Kemi-Tornion ammattikorkeakoululla tällä hetkellä käytössä olevat etäyhteydet on toteutettu VPN-tunneloinnilla. Kemi-Tornion ammattikorkeakoululla olevissa PC-asemissa käytössä on Windows XP- ja Windows 7 -käyttöjärjestelmät. /5/

Kemi-Tornion ammattikorkeakoulun tietoverkon asennuksesta ja hallinnasta on vastuussa IT-Lappia. IT-Lappia huolehtii kaikkien tukiasemien määrittelystä, asennuksesta sekä ylläpidosta. Tukiasemia ei ole luvallista asentaa ilman IT-Lappian hyväksyntää. Tästä poikkeuksena ovat kuitenkin opetuskäyttöön tarkoitetut laboratorioiden verkot, joiden käyttöönotosta on sovittava aina erikseen IT-Lappian kanssa. /5/

Kemi-Tornion ammattikorkeakoululla on olemassa oma tietoturvapolitiikkansa, joilla varmistetaan sisäinen tietoturva. Sen periaatteisiin kuuluvat:

- sisäinen verkko on erotettu internetistä rautapalomuurien avulla.
- liikenne palomuurin läpi on rajattu.
- sisäverkossa käytetään virustorjuntaohjelmistoa sekä sitä ylläpidetään ja päivitetään säännöllisesti.
- selainliikennettä (HTTP) ja sähköpostiliikennettä tarkkaillaan. /10/

3. SIEMENSIN OHJELMISTOT

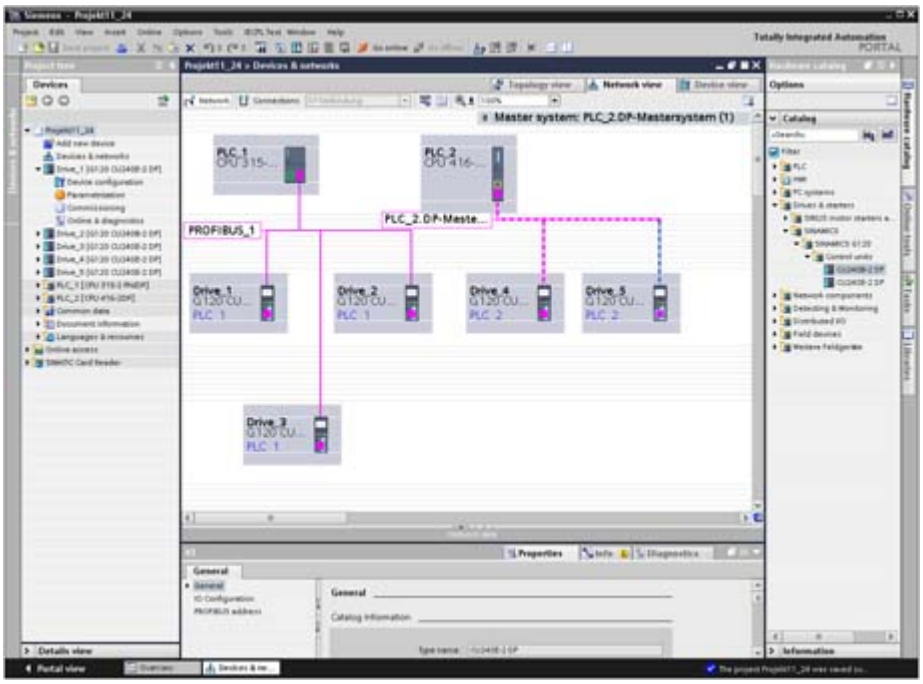
Laboratoriossa sijaitsevaa vesiprosessia ohjataan Siemensin S7-300 -logiikoilla (kuvassa 5), joita ohjelmoidaan Siemensin Simatic STEP 7 -ohjelmistolla. Lisäksi käytössä on WinCC-käyttöliittymäohjelmisto. Käytössä olevat ohjelmistoversiot ovat liitteessä 1. Kemi-Tornion ammattikorkeakoulun ulkopuolelta tapahtuvan ohjauksen toteuttamiseksi myös etäohjaus tulee tapahtumaan Siemensin ohjelmistoilla.

Kuva 5. Siemensin S7-300 -logiikka /13, s. 2./

3.1. TIA Portal

TIA Portal ei ole tällä hetkellä käytössä Kemi-Tornion ammattikorkeakoululla. TIA Portal (Totally Integrated Automation) on teollisuusautomaatiosuunnittelun ohjelmistoalusta, johon on yhdistetty suunnittelun tehostamiseksi ja nopeuttamiseksi logiikkaohjelmointi (Simatic STEP 7 V11), käyttöliittymäohjelmisto (Simatic WinCC V11) sekä myös väyläliitynnät. TIA Portaliin on integroitu lisäksi myös visualisointi sekä turvatekniikka. TIA Portal mahdollistaa siis useiden eri suunnitteluohjelmistojen käytön yhtä aikaa saman käyttöliittymän alla. Kuvassa 6 on esitetty TIA Portalin käyttönäkymää, jossa esimerkiksi

Siemensin S7-300 -logiikkaan on STEP 7 -ohjelmiston avulla yhdistetty Profibus-väylän kautta taajuusmuuttajia. /19/



Kuva 6. TIA Portalin käyttönäkymä /21/

Myös ulkoasu kaikissa TIA Portalin ohjelmistoissa on yhtäläinen. Täten TIA Portalilla on mahdollista toteuttaa sekä suunnittelu- että tuotantoprosessit kokonaiselle tuotantoketjulle. Tulevaisuudessa TIA Portal soveltuu myös moottorilähtöjen määrittämiseen. TIA Portal mahdollistaa myös automaation konfiguroinnin, diagnostiikan sekä ylläpidon samalla ohjelmalla. TIA Portalissa on mahdollista valita käyttöliittymän kieleksi saksa, kiina, englanti, italia, espanja tai ranska. /13/

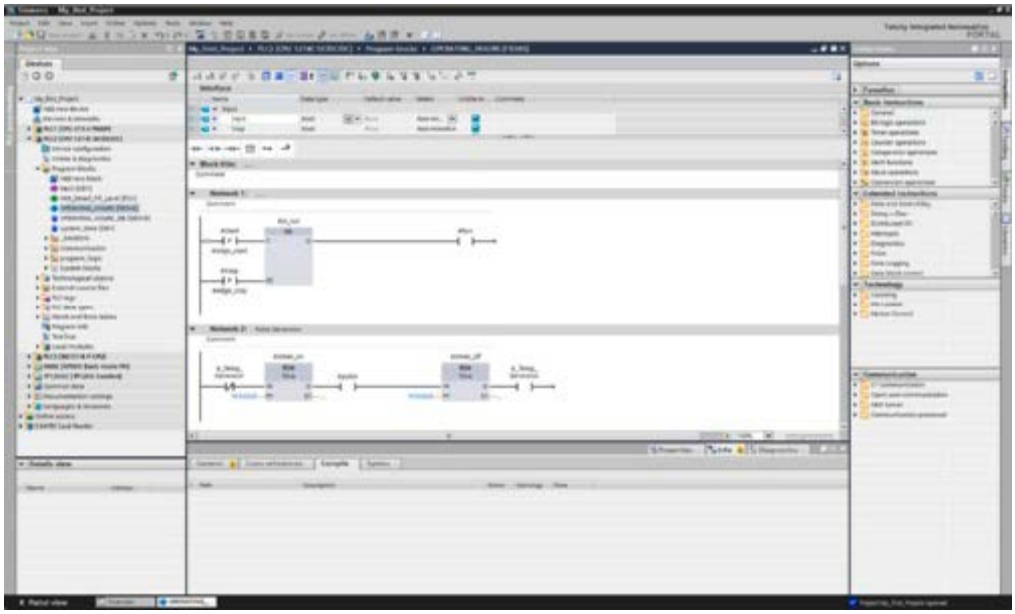
3.2. Simatic STEP 7

Siemensin STEP 7 -ohjelmistoa käytetään Siemens Simaticin ohjelmoitavien logiikoiden ohjausta ja ohjelmointia varten. Ohjelmalla luodaan järjestelmäkonfiguraatiot ja logiikkaohjelmat, jotka voidaan siirtää tietokoneelta laboratoriossa sijaitsevien S7-300 -logiikoiden kenttäyksiköihin MPI-väylän, tietokoneen sarjaportin tai USB-väylän avulla.

Luodut ohjelmat ja järjestelmäkonfiguraatiot tallentuvat keskusyksikön RAM-muistiin. /7 s.20 ja s. 23/

Laite- ja järjestelmäkonfiguraatioissa on laajennetulla diagnostiikalla varustettu graafinen verkkonäkymä sekä PC-asemien määrittelyssä Simatic IPC:den tuki. STEP 7 mahdollistaa myös Server/Client -yhteyksien graafisen määrittelyn. Käytettyjä IEC-ohjelmointikieliä ovat LAD (Relekaavio-ohjelmointi), FBD (Logiikkakaavio) sekä STL (käskylista). STEP 7 omaa myös ohjatut avusteet teknologiatoimintojen sekä kommunikaatiotoimintojen toteuttamisessa sekä mahdollistaa näppäimistöoikotien käytön. /13/

Käytettäessä Simatic Manageria on perusnäkymässä erilaisia ohjelmalohkoja, kuten OB1 ja FB1. Näihin on rakennettu järjestelmän erilaisia toimintoja. Simatic Managerilla pystytään luomaan myös aliohjelmia, ohjelmakutsuja sekä muuttujataulukoita. Simatic Managerilla pystytään myös konfiguroimaan tarvittava laitteisto sekä yleisesti hallinnoimaan projekteja (kuvassa 7) /7/

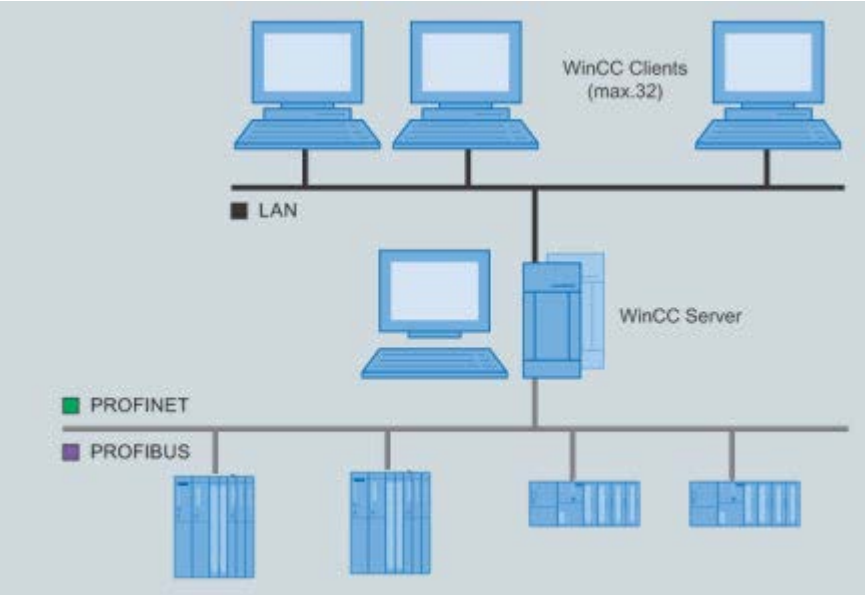


Kuva 7. STEP 7 -projekti /13/

3.3. Simatic WinCC

WinCC on käyttöliittymäohjelmisto, joka soveltuu kaikille HMI-sovelluksille ja on täydellisesti integroitu esimerkiksi juuri STEP 7 -ohjelmistoon, joten päällekkäisten määritelmien ja siten virheellisten syöttöjen mahdollisuudet on rajattu pois. WinCC-ohjelmistossa on yksi integroitu suunnitteluohjelmisto kaikille Simatic HMI -laitteille. /13/

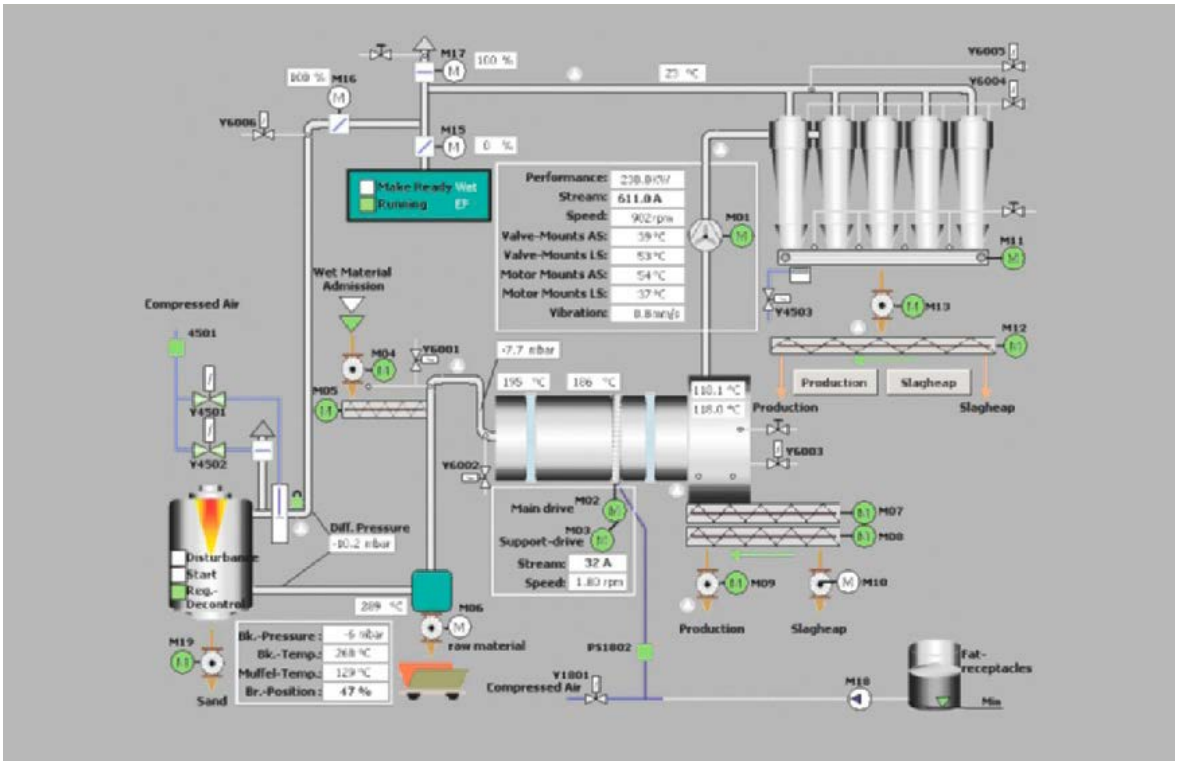
WinCC-ohjelmistoa voidaan käyttää myös Server/Client -sovelluksena eli käyttäjällä on mahdollisuus myös WinCC-sovellusten avulla etäohjata ja visualisoida prosessia samoilla ominaisuuksilla ja toiminnoilla kuin prosessin valvomossa esimerkiksi lähiverkon (LAN) välityksellä kuvan 8 mukaisesti. /9/



Kuva 8. Server/Client -toimintaperiaate /16/

Siemens Simatic WinCC -ohjelmistolla voidaan luoda selkeät ja helposti käytettävät operointinäytöt. Simatic WinCC -ohjelmistoon sisältyvä kirjasto sisältää tarvittavat graafiset komponentit, joiden avulla on helpotettu ja nopeutettu operointinäyttöjen luomista. /9/

Simatic WinCC Runtime -ohjelmistolla luodaan ja ohjataan kuvan 9 mukaisia operointinäyttöjä. PC-asemille Runtime-ohjelmistosta on saatavilla versiot Advanced ja Professional. Runtime-ohjelmisto on saatavilla myös ohjauspaneeleille. Simatic WinCC Runtime advanced -ohjelmisto kattaa PC-pohjaiset sovellukset operointiin ja monitorointiin yhden käyttäjän järjestelmissä, jotka ovat käytettävien laitteiden läheisyydessä. Simatic WinCC Runtime Professional -ohjelmisto puolestaan on PC-pohjainen visualisointi- ja SCADA-järjestelmä prosessien visualisointiin ja operointiin. /12, s. 16./



Kuva 9. WinCC Runtime -ohjelmiston operointinäyttö /13, s. 18./

4. TIETOTURVA

Tietoturvan tarkoituksena on suojata ulkopuolisilta Kemi-Tornion ammattikorkeakoululle tärkeät tiedot. Tietoturvan tavoitteena ovat lisäksi yksilön ja koko organisaation tietojen luotettavuus, oikeellisuus, käyttäjien tunnistaminen, pääsynvalvonta sekä tiedon helppo ja viiveetön käyttö. /8/

Teollisuusautomaatiossa tietoturvan haasteina ovat tietoturvan ylläpito sekä tietoturvauhkien jatkuva muutos. Tietoturvan kannalta olisi tärkeää saada yhteisymmärrys Kemi-Tornion ammattikorkeakoulun IT-organisaation, automaatio-osaston sekä myös automaatiolaitteiden toimittajien kesken. Käytännössä tätä haastetta voi lisätä esimerkiksi automaatiolaitteiden toimittajan toimipaikan sijainti eri paikkakunnalla. Lisähaasteena voidaan pitää myös eri tehtävien hoidon mahdollista ulkoistamista Kemi-Tornion ammattikorkeakoulun ulkopuolisille henkilöille tai yrityksille. /11/

Tietoturva voidaan jakaa kahteen eri kategoriaan:

- ennakoivalla tietoturvalla pyritään mahdollisimman hyvin estämään mahdolliset häiriöt.
- tietoturvahäiriöiden hallinnalla eli toimintaratkaisuilla varmistetaan järjestelmän toiminta häiriötilanteessa sekä toteutetaan häiriöstä aiheutuneet korjaavat toimenpiteet. /11/

4.1. Teollisuusautomaation tietoturvan hallinta

Teollisuusautomaatioon liittyvissä hankinnoissa on selvitettävä tarkoin tarvittavat tietoturvatoimenpiteet ja - ratkaisut. Tämä vaatii ymmärrystä automaatiojärjestelmien erityisvaatimuksista erityisesti kun käsitellään niiden liittämistä verkkoon. Hankintoja tehdessä sopimukset on luotava kattaviksi ja teollisuusautomaatiotoimituksista sovittaessa on selvennettävä:

- kaikkien osapuolten vastuut.
- toimintatavat, tiedotus ja tiedonvaihto.
- verkkotopologia ja liityntä verkkoon.
- virustorjuntaohjelmisto ja sen päivitykset.
- koventaminen.
- tietoliikenteen dokumentointi.
- käyttäjätunnukset ja salasanat.
- Kemi-Tornion ammattikorkeakoulun ja automaatiotoimittajan väliset tietoliikenneyhteydet .
- varmuuskopiointi ja tietojen palautus.
- Kemi-Tornion ammattikorkeakoulun muut IT-ratkaisut.
- langaton liikenne (WLAN). /11, s. 43-45./

Tietoturvan hallinta vaatii tietoturvatyön organisointia ja sekä Kemi-Tornion ammattikorkeakoulun eri henkilöstöryhmien kouluttamista ja ohjeistamista. Automaatioympäristössä tavoitteena on painottaa ennaltaehkäisevää tietoturvaa. Automaatiojärjestelmien tietoturvaperiaatteita ovat:

- suoran yhteyden estäminen automaatiojärjestelmiin muista tietoliikenneverkoista.
- ylimääräisten toimintojen rajaaminen pois eli tietojärjestelmäpalvelut määritetään ainoastaan automaatiojärjestelmän käyttöön.
- kriittisten tietojärjestelmien toiminnan seuraus.
- toipumissuunnitelma mahdollisten häiriöiden varalle.
- tietojärjestelmämuutosten ylläpidon organisointi. /11, s. 43-45./

4.2. Vaatimuksia automaatiojärjestelmän tietoturvalle

Toiminta reaaliaikaisessa prosessinohjausympäristössä ja korkeat vaatimukset käytettävyydelle aiheuttavat automaatiojärjestelmien tietoturvalle lisävaatimuksia, joten tavallisissa tietojärjestelmissä käytetyt tietoturvaratkaisut eivät sellaisenaan sovellu automaatiojärjestelmiin. Automaatiojärjestelmillä tietoturvatason tulee olla korkeampi,

sillä ne ovat vakiintuneempia suhteessa esimerkiksi toimistojärjestelmiin. Automaatio-alan organisaatioissa tunnetaan laitteisto paremmin ja laitteisto myös pysyy käytössä pidempään. Automaatiojärjestelmissä konfiguraatiota muutetaan yleensä ainoastaan suurempien kunnossapito- ja muutostöiden yhteydessä. Automaatiojärjestelmissä ei yleensä ole liiketoiminnan kannalta salassapidettävää tietoa eikä suoraa yhteyttä internetiin välttämättä tarvita. Kuitenkin tässä tapauksessa etäyhteyden muodostamiseksi internet-yhteyden muodostaminen on välttämätöntä. Automaatiojärjestelmissä pääsyn hallinta on tarkemmin suunniteltu ja rajattu sekä henkilöstö on koulutettu kyseisiin tehtäviin. /11 s.68/

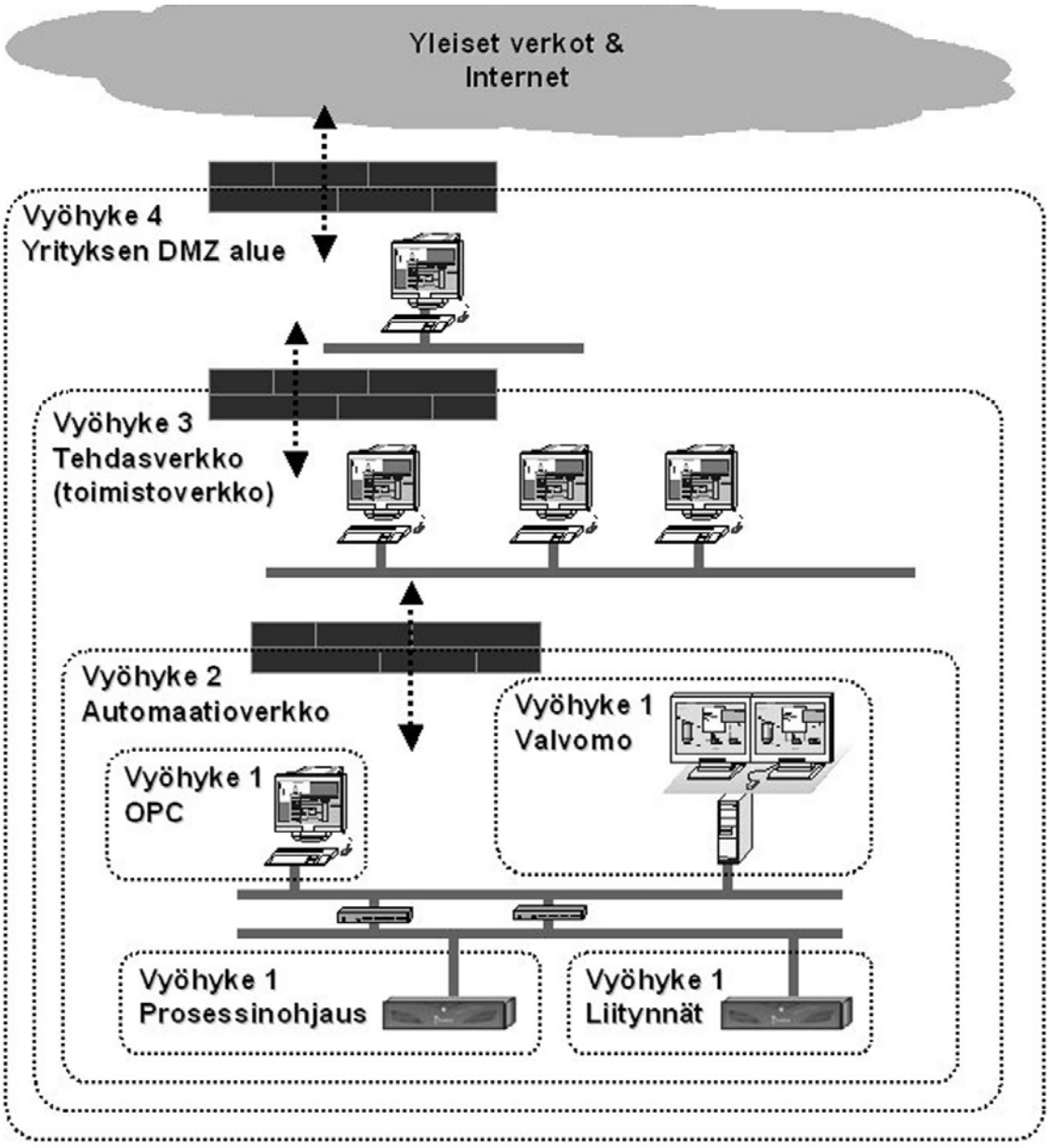
Tietoturvaa täytyy tutkia lähinnä riskienhallinnan kannalta, sillä täydellistä tietoturvaa ei voi saavuttaa. Tästä johtuen onkin pyrittävä hahmottamaan tässä tapauksessa hyväksyttävä tietoturvataso, jossa otetaan huomioon ohjattavan vesiprosessin reaaliaikaisuus sekä tarvittavat tietoliikenneyhteydet. Valitut tietoturvaratkaisut ja työn suorittajat vaikuttavat oleellisesti tietoturvatasoon sekä siihen, kenellä on vastuu mahdollisien vahinkojen ja häiriöiden tapahtuessa. /11/

Automaatiojärjestelmä tulee suunnitella siten, että se sietää ja havaitsee mahdollisimman hyvin virhetoimintoja sekä häiriötilanteesta toipuminen on nopeaa. Häiriöitä ei voida kuitenkaan kokonaan estää, joten mahdolliset häiriöt ja vahingot olisi pyrittävä rajaamaan mahdollisimman vähäisiksi. /11/

Yksittäiset ratkaisut eivät pysty antamaan riittävää tietoturvaa, joten tiedon turvaamiseen tulisikin käyttää useita toisiaan täydentäviä ratkaisuja. Kaikkien ratkaisuiden tulee olla asianmukaisesti suunniteltuja, toteutettuja sekä ylläpidettyjä. Tämä niin sanottu syvyyssuuntainen malli on esitetty kuvassa 10. Siinä useaan eri vyöhykkeeseen sijoitetut tietoturvaratkaisut auttavat saavuttamaan tehokkaamman tietoturvan. Suojausmenetelmät voivat sisältää teknisten ratkaisuiden myös lisäksi esimerkiksi ohjeita ja koulutusta. /11, s. 69./

Kuvan 10 mukaisesti automaatioverkko tulee olla erotettuna omaksi verkkosegmentikseen Kemi-Tornion ammattikorkeakoulun muusta verkosta. Verkkojen erotukseen sopivat erilliset palomuurit tai reititinpalomuurit. Segmentointi suojaa automaatiojärjestelmää

toisaalla verkossa tapahtuvilta häiriöiltä sekä vioilta ja näin voidaan varmistaa käytettävän prosessin häiriötön toiminta. Yksi tapa on esimerkiksi luoda automaatioverkon sekä Kemi-Tornion ammattikorkeakoulun sisäverkon välille suoja-alue (DMZ), joka on suojattu palomuureilla sekä automaatio- että sisäverkossa. /11, s. 79./



Kuva 10. Segmentointi /11, s. 69./

4.3. Tekniset menetelmät - ja ratkaisut

Useimmilla automaatiotoimittajilla on olemassa omat määritelmänsä ja ratkaisunsa automaatiojärjestelmiensä ja laitteidensa tietoturvalle. Automaatiotoimittajien tietoturvaperiaatteet saattavat kuitenkin poiketa Kemi-Tornion ammattikorkeakoulun toimintatavoista tietoturva-asioissa. Automaatiotoimittajien, Kemi-Tornion ammattikorkeakoulun IT- ja automaatio-osastojen tulisi yhteistyössä sovittaa yhteen tietoturvaperiaatteet, jolloin voidaan saavuttaa niin vesiprosessin korkea käytettävyys kuin haluttu tietoturvatasokin. Ilman yhteistyötä voi ilmetä ristiriitoja tietoturva-asioissa, mistä voi taas ilmetä ongelmia automaatiojärjestelmän sekä vesiprosessin toiminnassa. Vesiprosessin käytettävyyden riskejä voidaan rajoittaa ja vähentää tietoliikenneverkkojen segmentoinnin lisäksi ratkaisujen vakioinnilla sekä koventamisella eli hardenoinnilla. /11/

Ratkaisujen vakioinnilla tarkoitetaan valittujen ratkaisujen ja osien pitämistä muuttumattomana järjestelmän koko elinkaaren ajan, mutta on mahdollista, että Kemi-Tornion ammattikorkeakoulun ja automaatiotoimittajan kesken voi kuitenkin ilmetä ristiriitoja liittyen tietoturva-asioihin. /11/

Koventamisella tarkoitetaan tässä tapauksessa automaatiojärjestelmässä tarvitsemattomien ja ylimääräisten ohjelmistojen, osien ja toimintojen käytön estämistä käytössä olevista PC-asemista. Koventamista voidaan käyttää lähes kaikkiin järjestelmän osiin, mutta yleisimpiä käyttökohteita ovat PC-työasemat – ja palvelimet. Lisäksi koventamista voidaan toteuttaa itse automaatioverkossa. /11/

Koventaminen tulee suorittaa järjestelmälle aina ennen käyttöönottoa ja se onkin normaali toimenpide toimitettaessa uusia automaatiolaitteita ja -järjestelmiä. Uusimpiin automaatiojärjestelmiin on saatavilla tietoturvaratkaisuja valmistajienkin puolelta, mutta on mahdollista, ettei vanhemmissa automaatiojärjestelmissä ja -laitteissa voi välttämättä käyttää esimerkiksi virustorjuntaohjelmistoja. /11/

4.4. Suojausmenetelmät

Yleisiä suojausmenetelmiä ovat tekninen, hallinnollinen sekä fyysinen tietoturva. Teknisen tietoturvan tarkoituksena on se, ettei käytetyissä laitteissa ja ohjelmistoissa ole tietoturvapuutteita. Tarvittava tietoturva tulee olla mietittynä tarkkaan jo ennen laitteiden ja ohjelmistojen hankintapäätöstä. Tietojärjestelmiin pääsyä tulee valvoa salasanojen- ja käyttäjätunnusten avulla, joten voidaan valvoa, kenellä on oikeus päästä käsiksi mihinkin tietoihin. Jotta voidaan estää ulkopuolisten pääsy tietoverkon sisältöön, on mahdollista käyttää varmistuskeinona palomuurien lisäksi esimerkiksi käytettävän tiedon kryptaamista. /8/

Fyysinen tietoturva tarkoittaa esimerkiksi suljetussa huoneessa tai rakennuksessa sijaitsevia tietokoneita tai tietoa. Lukitulla tilalla varmistetaan, ettei ulkopuolinen henkilö pääse käsiksi tietokoneisiin, kovalevyihin tai muihin tiedontallennuslaitteisiin. /8/

Hallinnollinen tietoturva tarkoittaa organisaation ja sen työntekijöiden riittävää tietoturvaosaamista. Organisaation ja sen työntekijöiden tulee ymmärtää esimerkiksi salasanojen käytön merkitys ja niiden vastuullinen käyttö. Salasanoja ei saa säilyttää ulkopuolisten henkilöiden ulottuvilla. Salasanojen huolellinen käyttö pienentää huomattavasti riskiä tietoturvavuotoihin. /8/

4.5. Tekninen suojaus

Teknisen suojauksen menetelmiä ovat palomuurit, salausprotokollat sekä varmenteet. Palomuurin tarkoituksena on estää asiattoman liikenteen pääsy yksityisestä verkosta julkiseen ja päinvastoin. Palomuurilla torjutaan myös tietokoneviruksia sekä osoitteen väärennöksiä. Palomuuriin sisältyy yleensä liikennettä valvova reititin ja Proxy-palvelin. Reititin tarkistaa jokaisen palomuurin kautta tulevan IP-paketin ja joko sallii tai estää läpikulun. Proxy-palvelimen tehtävänä on tunnistaa käyttäjä ja huolehtia tietojen kirjaamisesta. Palvelin tarkistaa käyttäjätunnuksen ja salasanan avulla käyttäjän oikeudet suojattuihin kohteisiin. /2/

Palomuuri on edelleen tarpeellinen, mutta sen merkitys on vähentynyt tietoturvan kokonaisuudessa. Palomuuri ei pelkästään riitä suojaamaan yritystä, sillä sen ohittamiseen on olemassa myös muita reittejä. Palomuuri toimii kuitenkin suojana lähinnä hakkereilta ja haittaohjelmia vastaan sen hyöty on suhteessa vähäisempi. Palomuuri ei pysty erottamaan, onko työasemasta tuleva yhteys avattu tarkoituksella vai käyttäjän tietämättä. /2/

Palomuurit voivat olla joko erillisiä laitteita (Rautapalomuurit) tai tietokoneessa toimivia ohjelmia (Softapalomuurit). Rautapalomuuri on toimivin ja luotettavin vaihtoehto yrityskäyttöön. Rautapalomuuriin on käytännössä mahdoton murtautua ja erillisenä laitteena se toimii, vaikka itse tietokoneessa ilmenisikin ongelmia. Yksi laite riittää suojaamaan koko sisäverkon, joten siihen kuuluviin tietokoneisiin ei tarvitse erikseen tehdä säätöjä. Suojaus voidaan myös näin keskittää yhteen paikkaan, mikä helpottaa tietoturvan ylläpitoa. /2/

Rautapalomuurit (kuvassa 11) vaativat osaavan ylläpitohenkilön. Rautapalomuurit eivät myöskään pysty antamaan reaaliaikaisia ilmoituksia käyttäjälle lähtevästä liikenteestä. Palomuuri ottaa vastaan internetistä tulevat VPN-yhteydet ja sallii pääsyn sisäverkkoon. Tämän ansiosta käyttäjät voivat tehdä esimerkiksi etätyötä kotonaan, työmatkalla, tai tässä tapauksessa ohjaamaan vesiprosessia käyttäen Kemi-Tornion ammattikorkeakoulun sisäverkkoa. /2/

Kuva 11. Rautapalomuuri /16/

VPN eli Virtual Private Network on tekniikka, jolla voidaan luoda luotettava ja salattu yhteys kahden eri verkon välille tai mahdollisesti tietokoneen ja verkon välille. Tällä menetelmällä käyttäjän ei tarvitse itse huolehtia suojauksesta, vaan laitteisto tekee sen itse. Virtual Private Networkin ei yleensä vaadi muutoksia sovelluksiin, verkkokomponentteihin tai muillekaan tietoliikennetasoille. /2/

SSL (Secure Socket Layer) on salausprotokolla, jolla salataan tunnistus palvelimen ja käyttäjän välillä. Sillä voidaan tunnistaa palvelin ja neuvotella tietoliikenteessä käytettävästä salauksesta. SSL-salausprotokollaa käytetään esimerkiksi pankkipääteyhteyksien suojauskeinona. Merkkinä SSL-varmenteen toiminnasta selaimessa näkyy lukon kuva ja joissain selaimissa esimerkiksi osoitekentän väri muuttuu. SSL-varmenne käytännössä siis estää ulkopuolisia näkemästä nettiliikenteen tapahtumia. /8/

Yhtä tärkeää on myös www-palvelun todentaminen eli autentikointi. Lukon kuva selaimessa kertoo, että selain on tarkistanut www-palvelun aitouden ja sen jälkeen muodostanut salatun yhteyden. Palvelun aitouden tarkistamiseen tarvitaan kuitenkin sertifikaatti eli sähköinen henkilötodistus. Jokin taho on ensin tarkistanut palvelun aitouden ja sen jälkeen myöntänyt sille todistuksen, jonka selain tarkistaa ja hyväksyy. Jos varmenne havaitaan vääräksi, antaa selain siitä varoituksen. Varmenne on sidottu IP- ja www-osoitteisiin ja se on lukittu salaustekniikalla niin, ettei ulkopuolinen pysty muuttamaan sen sisältöä. Käyttäjä ei pysty itse vaikuttamaan SSL:n toimintaan. SSL kytkeytyy päälle automaattisesti, jos palvelimella on varmenne. Varmenteen puuttuessa myöskään SSL:ää ei voi käyttää. /2/

4.6. Virustorjunta

Hakkeroinnin lisäksi uhkana Kemi-Tornion ammattikorkeakoululle ovat tietokonevirukset, jotka ovat pienikokoisia haittaohjelmia, jotka voivat levitä internet-selaimen kautta, sähköpostien liitetiedostoina tai esimerkiksi CD-ROMien kautta tietokoneelta toiselle. Yleisin ja suurin viruksien aiheuttama vahinko on tietojen katoaminen. Virus voi tyhjentää

kiintolevyn, mutta sen tiedot ovat kuitenkin palautettavissa. Virus saattaa myös sotkea tietokoneen muistin ja aiheuttaa käyttöjärjestelmän häiriöitä, jolloin tietokone saattaa esimerkiksi kaatuilla jatkuvasti. Tietokonevirukset voivat aiheuttavaa myös yhteensopivuusongelmia, koneen toiminnan hidastumista sekä tiedostojen tuhoutumista. /8/

Tietokoneviruksia vastaan tehokkain toiminta on ennaltaehkäisevä tietoturva eli virustorjuntaohjelmiston sekä palomuurin käyttö, jotka vaikeuttavat virusten toimintaa ja estää niiden sisäänpääsyä järjestelmään. Virustorjuntaohjelmiston taustasuojaus tulisi pitää myös aktiivisena. Tietojärjestelmään ei tule myöskään asentaa tuntemattomia tai epäilyttäviä ohjelmistoja tai tiedostoja. Tietojärjestelmästä kannattaa myös ottaa säännöllisin väliajoin varmuuskopiot. /8/

4.7. Avaimet ja pääsynhallinta

Kahden eri paikan välisen tiedonsiirron turvaamiseksi on olemassa kaksi eri menetelmää. Salaisen avaimen menetelmässä viestin salaaminen ja avaaminen tapahtuu samalla avaimella. Menetelmän heikkoutena on se, miten avain saadaan kaikille käyttäjäosapuolille ilman sen päätymistä myös ulkopuolisten henkilöiden haltuun. Vahvuutena on siirtonopeus, eli sillä voidaan suojata suuria tietomääriä siirtonopeuden kärsimättä. /8/

Julkisen avaimen menetelmässä olisi käytössä kaksi eri avainta, salainen ja julkinen. Viesti salataan vastaanottajan julkisella avaimella ja viesti puretaan salaisella avaimella. Julkinen avain voidaan antaa osapuolelle, jonka kanssa on tarpeen vaihtaa tietoja julkisesti. Heikkoutena verrattuna salaiseen avaimen-menetelmään on siirtonopeuden hitaus. /8/

5. SIEMENSIN RATKAISUT ETÄOHJAUKSEN TOTEUTTAMISEKSI

Siemensillä on etäohjauksen toteuttamiseksi vaihtoehtoina Simatic WinCC WebNavigator sekä Simatic WinCC Sm@rtServer. Molemmat perustuvat Server/Client -yhteyteen, mutta toimivat kuvan 12 mukaisesti Simatic WinCC Runtimen eri ohjelmistoversioissa. Lisäksi etäohjauksen toteuttamiseksi Siemensillä on tarjota Telecontrol Service, mutta Kemi-Tornion ammattikorkeakoulun laboratoriossa käytössä oleviin S7-300 -logiikoihin Telecontrol Service ei sovellu, joten vaihtoehtona on hankkia Telecontrol Servicen lisäksi joko S7-1200 -logiikat varustettuna CP 1242-7 -modeemilla tai S7-200 -logiikat SINAUT MD720-3 -modeemilla varustettuna. Siemensillä on myös tarjolla tarvittavat tietoturvaratkaisut. /1/

Option	Panel Runtime (device-dependent)	WinCC Runtime Advanced	WinCC Runtime Professional
WinCC Logging	●	○	●[1)]
WinCC Recipes	●	○	○
WinCC Audit	○	○	–
SIMATIC Logon	○	○	●
WinCC Sm@rt Server	○	○	–
WinCC Client	–	–	○
WinCC Server	–	–	○
WinCC WebNavigator	–	–	○
WinCC DataMonitor	–	–	○

● included ○ optionally available

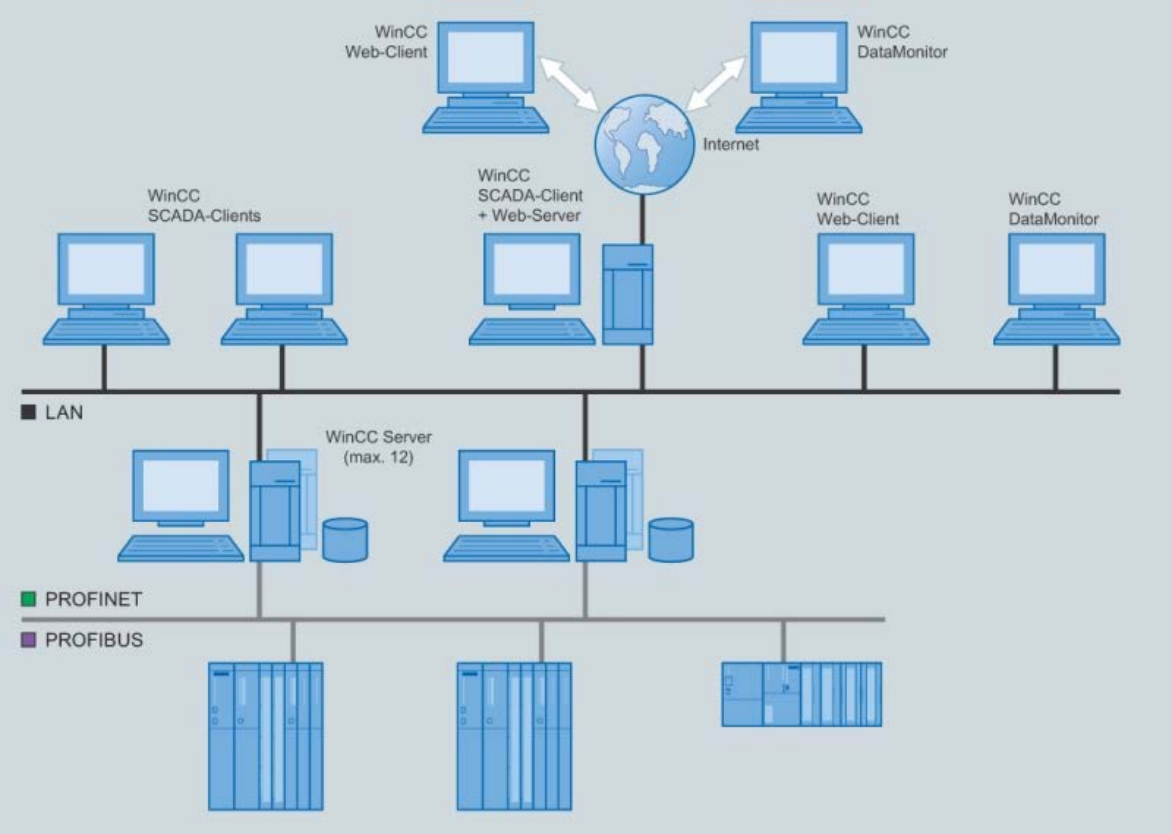
Kuva 12. WinCC Runtime -ohjelmiston sovellukset /13, s. 21./

5.1. Simatic WinCC WebNavigator

Simatic WinCC WebNavigator on WinCC-sovellus, joka tarjoaa mahdollisuuden ohjata vesiprosessia etäkäyttöasemalta samalla tavoin kuin sitä ohjaisi paikanpäällä Kemi-Tornion ammattikorkeakoulun laboratoriossa. Simatic WinCC WebNavigator vaatii toimiakseen ohjelmiston WinCC Runtime Professional sekä käyttöliittymäksi ohjelmiston WinCC. /13 s26, 21/

5.1.1. Toiminta

Simatic WinCC WebNavigator mahdollistaa vesiprosessin ohjauksen internetin, intranetin sekä lähiverkon (LAN) kautta ilman, että WinCC-projekteihin tarvitsee tehdä muutoksia. Täten Simatic WinCC WebNavigator mahdollistaa etäkäyttäjän pääsyn WinCC-palvelimen tietokantaan käytännössä mistä tahansa. /14, s. 26./



Kuva 13. Simatic WinCC WebNavigatorin mahdolliset käyttötavat /15/

Kuvassa 13 on esitetty erilaiset käyttömahdollisuudet. Vesiprosessin ohjaus ja valvonta tulee Kemi-Tornion ammattikorkeakoulun ulkopuolelta tapahtumaan tässä tapauksessa internetin kautta, jolloin haluttuja WinCC- projekteja voitaisiin selata ja käyttää yhtä aikaa verkkoselaimen eri välilehdissä käytettäessä verkkoselainta, jossa on MultiTab-toiminto (kuvassa 14). Simatic WinCC WebNavigator mahdollistaisi jopa 50 yhtäaikaista etäohjausasemaa missäpäin maailmaa tahansa. Simatic WinCC WebNavigator tarvitsee toimiakseen kuvan 13 mukaisesti käytössä oleviin S7-300 -logiikoihin Profinet-kortit.

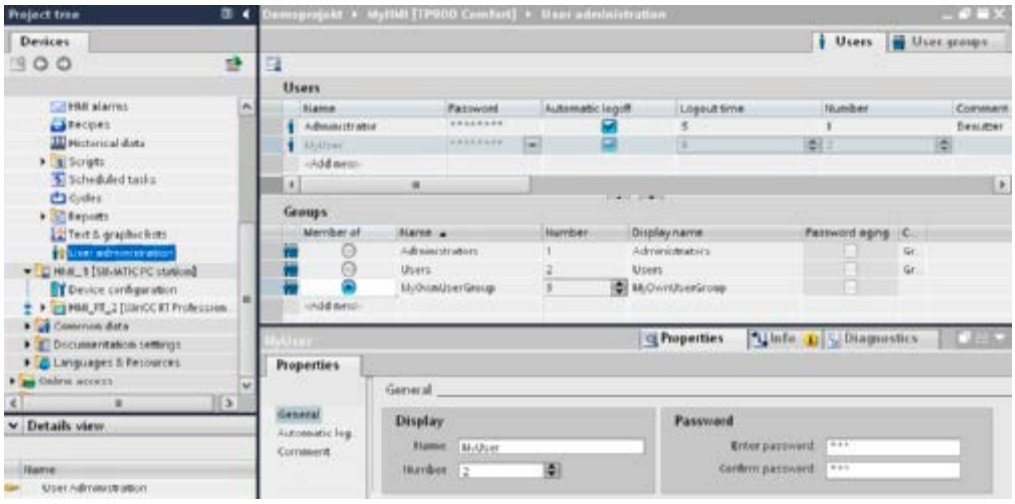
WebNavigatorin käyttöä helpottaa se, ettei etäkäyttöasemiin tarvitse olla asennettuna WinCC-ohjelmistoja. /13, s. 26./

Kuva 14. Simatic WinCC WebNavigatorin MultiTab-toiminto /15/

5.1.2. Pääsynhallinta ja suojaus

Internetin kautta käytettävät etäkäyttöasemat on mahdollista suojata käyttäjätunnuksilla ja salasanoilla sekä käyttöoikeuksia voidaan rajoittaa käyttäjäryhmien, kuten esimerkiksi opiskelijoiden ja henkilökunnan mukaan. Opiskelijoiden käyttöoikeus voitaisiin näin rajata esimerkiksi vesiprosessin osittaiseen ohjaamiseen tai pelkkään monitorointiin. /13, s. 26.)

Käyttöoikeuksien rajoittaminen on mahdollista toteuttaa myös esimerkiksi Simatic Logonin avulla. Jokaisesta sisään – ja uloskirjautumisesta jää jälki, joten ohjelmistoa käyttäneet henkilöt sekä mahdolliset, mutta epätodennäköiset väärinkäytöt tai luvattomat tunkeutumiset on myös mahdollista selvittää. Kuvassa 15 on esitetty käyttöliittymän näkymä, jossa käyttöoikeuksia voidaan määrittää. WebNavigator myös mahdollistaa turvallisen ja korkean käytettävyyden toisistaan erotetuilla Web- ja WinCC-serverillä. /13, s. 26./



Kuva 15. Pääsynhallinta ja käyttöoikeuksien määrittäminen /13, s. 18./

5.1.3. Käyttökohteet

WebNavigator sopii hyvin sovelluksiin, jotka on toteutettava minimikustantein sekä hyvin myös käyttökohteisiin, joissa prosessi on rakentunut eri osiin laajalle alueelle. Simatic WinCC WebNavigator on käytössä esimerkiksi useissa vedenkäsittelylaitoksissa ympäri maailmaa. Simatic WinCC WebNavigatoria voitaisiin käyttää etäkäytön lisäksi myös vesiprosessin normaalina ohjaustapana Kemi-Tornion ammattikorkeakoululla. /13, s. 26./

Hyödyt:

- prosessin ohjaus ja monitorointi ympäri maailmaa.
- nopea päivitys.
- pienet ylläpitokustannukset.
- korkea käytettävyys ja sen turvallisuus.
- korkea tietoturva. /13, s. 26./

5.1.4. Lisenssit

Siemensin WebNavigatorin lisenssiä voidaan asentaa etäkäyttöasemille rajattomia kertoja. Vastaavasti tarvitaan kuitenkin serveri-pohjainen lisenssi, jotta voidaan käyttää Kemi-Tornion ammattikorkeakoululle tulevaa WebNavigator-palvelinta. Lisenssejä on mahdollista hankkia 3, 10, 25 tai 50:lle etäkäyttöasemalle. Verkkolaitteita on mahdollista päivittää ja etäkäyttöasemien määrää voidaan tulevaisuudessa lisätä myös tarvittaessa. /13, s. 26./

5.1.5. Tarvittavat järjestelmät, ohjelmistot ja palvelut

Simatic WinCC WebNavigatorin hankinnassa tulee ottaa tarvittavien ohjelmistojen ja palveluiden lisäksi ottaa huomioon myös tarvittavat järjestelmävaatimukset, kuten Windows-käyttöjärjestelmien yhteensopivuus hankittavien ohjelmistojen kanssa. Tarvittavat tietoturvapalvelut on esitetty liitteessä 1. /13, s. 11./

Yhteensopivat käyttöjärjestelmät:

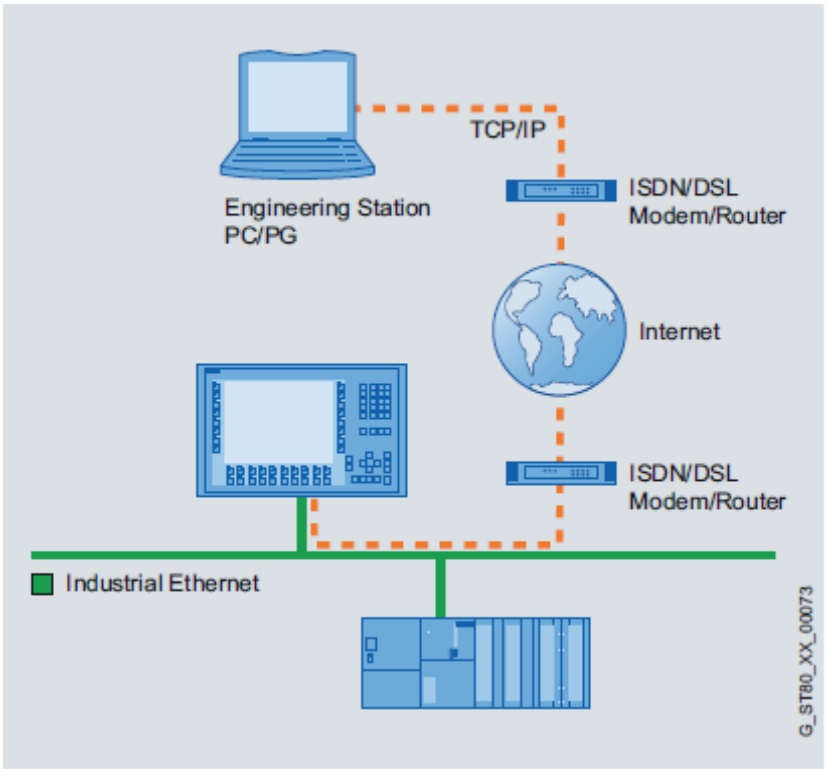
- Windows XP Professional SP3 (32bit).
- Windows 7 Professional/Enterprise/Ultimate (32/64bit).
- Windows 7 Professional/Enterprise/Ultimate SP1 (32/64bit). /13, s. 11./

Tarvittavat ohjelmistot ja palvelut:

- Siemens Simatic WinCC -ohjelmisto.
- Simatic WinCC WebNavigator -ohjelmisto.
- Simatic WinCC Runtime Professional -ohjelmisto.
- tietoturvapalvelut. /14/

5.2. Simatic WinCC Sm@rtServer

WinCC Sm@rtServer mahdollistaa Simatic HMI -järjestelmien etäohjauksen ja etävalvonnan mistä tahansa internetin, sisäverkon tai intranetin kautta (kuvassa 16). Sm@rtServer mahdollistaa myös eri osaprosessien ohjauksen eri paikoista. WinCC Sm@rtServer toimii ohjelmistoversiossa WinCC Runtime Advanced ja vaatii WebNavigatorin tavoin käyttöliittymäksi Simatic WinCC:n, josta on mahdollista käyttää eri ohjelmistoversioita. /13, s. 24/

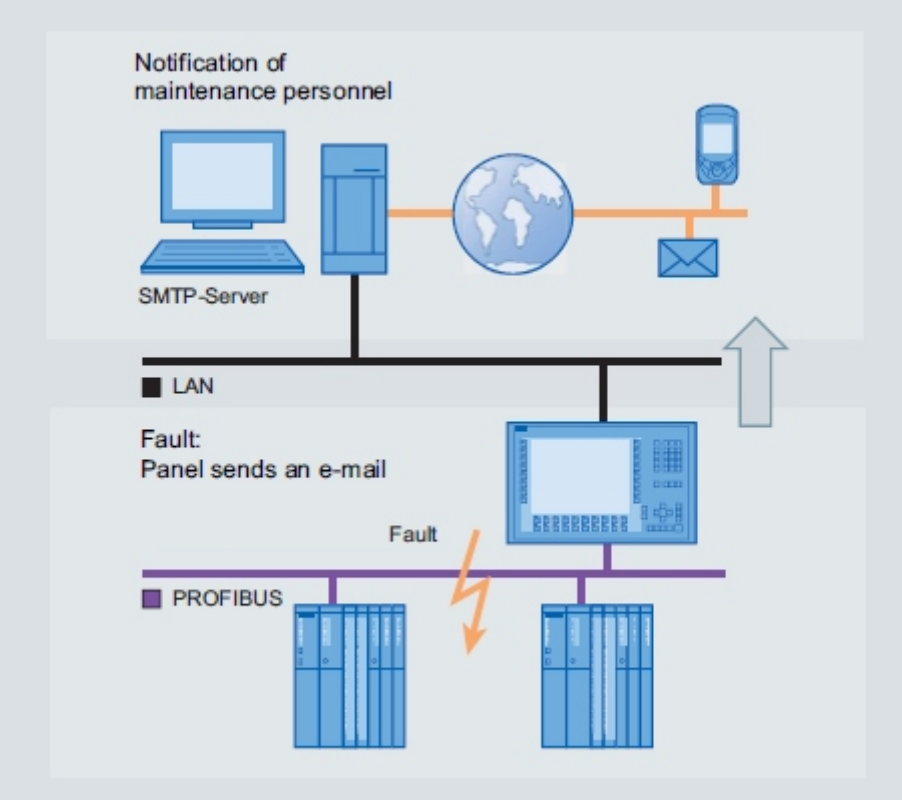


Kuva 16. Etäohjaus /14, s. 24./

5.2.1. Toiminta

Simatic WinCC Sm@rtServerin avulla on mahdollista luoda yhteensä 32 etäohjausasemaa, joista yhtäaikaisesti käytössä voi olla viisi. Ohjauspaneeleita Sm@rtServerillä voi olla yhtä aikaa käytössä kolme. WinCC Sm@rtServeriä voidaan käyttää kahdella eri tavalla. Mahdollista on käyttää joko Sm@rtClient-konseptia, jolloin prosessin ohjaus- ja valvomonäyttöihin pääsee käsiksi etäkäyttöaseman kautta tai toisena vaihtoehtona käyttää

internet-selainta, kuten Internet Exploreria. Lisäksi voidaan käyttää lähiverkkoa (LAN) kuvan 17 mukaisesti. WinCC Sm@rtServerillä on myös mahdollista toteuttaa myös vikailmoitusten välittäminen esimerkiksi tekstiviestipohjaisilla ratkaisuilla. /13, s. 24./



Kuva 17. Etäohjaus lähiverkon kautta /20/

Serverin toiminta on yksinkertaista kytkeä päälle laitteiston asetuksista sekä käyttöliittymän näyttö voidaan asettaa siten, että sitä voidaan joko ohjata tai ainoastaan monitoroida. Sm@rtServerillä voidaan kuitenkin toteuttaa myös koko prosessin ohjaus sekä voidaan asettaa halutulle etäohjausasemalle täydet käyttöoikeudet. /13, s. 24./

Hyödyt:

- mahdollistaa jaetut käyttöasemat suurillekin prosesseille, jotka ovat jakaantuneet isolle alueelle.
- joustava ratkaisu etäohjaukseen mistä tahansa.
- mahdollistaa palveluntarjoajan sekä kunnossapidon henkilöstön pääsyn järjestelmään mistäpäin maailmaa tahansa. /13, s. 24./

5.2.2. Pääsynhallinta ja suojaus

Samoin kuin Simatic WebNavigatorissa, myös Sm@rtServerin pääsynhallintaa voidaan rajoittaa käyttäjätunnusten, henkilötietojen ja salasanojen avulla. Simatic Logon on mahdollista hankkia myös Simatic Sm@rtServeriin. Pääsynhallinnan rajoituksien määrittämisen käyttöliittymänäkymä on yhtäläinen WebNavigatorin kanssa ja se on esitetty kuvassa 14. /13, s. 18./

Eri käyttäjäryhmillä tulee olla eritasoiset käyttö- ja pääsyoikeudet prosessin eri toimintoihin. Prosessin ja ohjelmistojen hallinnointiin tarvitaan luonnollisesti erityisosaamista, joten etäkäyttäjille on mahdollista asettaa rajoitetut käyttöoikeudet etäohjauksen yhteydessä. /13, s. 18./

5.2.3. Tarvittavat järjestelmät ja ohjelmistot

Hankittaessa Simatic WinCC Sm@rtServeriä tulee ottaa huomioon käyttöjärjestelmien yhteensopivuus. Simatic WinCC toimii käyttöjärjestelmissä Windows XP ja Windows 7. Tarvittavat tietoturvapalvelut on esitetty liitteessä 1.

Yhteensopivat käyttöjärjestelmät:

- Windows XP Professional SP3 (32bit).
- Windows 7 Professional/Enterprise/Ultimate (32/64bit).
- Windows 7 Professional/Enterprise/Ultimate SP1 (32/64bit). /13, s.11./

Tarvittavat ohjelmistot ja palvelut:

- Siemens Simatic WinCC-ohjelmisto.
- Simatic WinCC Runtime Advanced-ohjelmisto.
- Simatic Sm@rtServer-ohjelmisto.
- tietoturvapalvelut. /13/

5.3. Siemensin tietoturvapalvelut

Siemensillä on myös tarjota tarvittavat tietoturvapalvelut, joihin kuuluvat palomuuri ja DMZ-palvelu, Virustorjunta, Whitelisting-palvelu sekä WSUS- ja Patch Management -palvelu. Myös tarvittavat tietoturvapalvelut on kannattavaa hankkia samalta automaatiotoimittajalta päällekkäisten määritelmien estämiseksi sekä tietoturvan varmistamiseksi. /19/

Palomuuri ja DMZ-palveluihin sisältää järjestelmäarkkitehtuurin tietoturvallisen suunnittelun sekä toteutuksen. Tämän palvelun avulla voidaan segmentoida verkon toiminnalliset osat sekä voidaan hallita verkkojen välistä liikennettä. Palvelu sisältää teknisen määrittelyn ja dokumentoinnin, tarvittavat laitteet ja ohjelmistot FAT- ja SAT-testauksen, palomuurin asennuksen ja sen testauksen sekä koulutusta. /19/

Siemensin virustorjuntapalvelu sisältää virustorjunnan suunnittelun, asennuksen ja käyttöönoton. Myös virustorjuntaohjelmiston virustunnisteet päivittyvät automaattisesti, joten ohjelmiston käyttö ja ylläpito on selkeää. Virustorjunta sisältää teknisen määrittelyn ja dokumentoinnin, tarvittavat laitteet ja ohjelmiston ja sen hallintakonseptin asennuksen ja hallinnan, FAT- ja SAT-testauksen sekä myös uusimpien virustunnisteiden asennuksen ja koulutusta virustojuntaohjelmiston käyttöön. /19/

Whitelisting-palvelun avulla voidaan luoda lista sallituista ohjelmistoista sekä palveluista eli suorittaa automaatiojärjestelmän koventaminen. Palvelut sekä ohjelmistot, jotka eivät ole sallittavien listalla, eivät siis ole suoritettavissa. Whitelisting on suoja haittaohjelmia vastaan, jotka voivat levitä tietokoneille esimerkiksi USB-muistitikkujen kautta. Palvelu

sisältää teknisen määrittelyn sekä dokumentoinnin, tarvittavat laitteet – ja ohjelmistot, palvelu asennuksen ja hallinnan, FAT- ja SAT-testauksen ja koulutusta. /19/

WSUS- ja Patch Management -palvelu käsittää tietoturvapäivitysten suunnittelun, asennuksen sekä myös käyttöönoton. Tietoturva varmistetaan Siemensin sekä myös Microsoftin ajan tasalla olevilla tietoturvapäivityksillä. Palvelu sisältää teknisen määrittelyn ja dokumentoinnin, tarvittavat tietoturvalaitteet ja ohjelmistot, päivitysten hallintakonseptin asennuksen sekä hallinnan, SAT- ja FAT-testauksen ja myös koulutusta /19/

6. RATKAISU VESIPROSESSIN ETÄOHJAUKSEN TOTEUTTAMISEKSI SIEMENSIN OHJELMISTOILLA

Toteutusratkaisuun on luotu hankintaesitys sekä käyttöönottosuunnitelma. Hankintaesityksessä on esitetty valittu ratkaisu, miksi valittuun ratkaisuun päädyttiin sekä eri vaihtoehdot sen toteuttamiseksi. Käyttöönottosuunnitelmaan on luotu suunnitelma valitun ratkaisun käyttöönottamiseksi sisältäen asennuksen, testauksen ja ylläpidon.

6.1. Hankintaesitys

Kemi-Tornion ammattikorkeakoulun automaatiolaboratoriossa sijaitsevan vesiprosessin etäohjauksen toteuttamiseksi esitetään hankittavaksi Simatic WinCC WebNavigator. Valittuun ratkaisuun päädyttiin WebNavigatorin monipuolisuuden takia. Lisäksi etäohjauksen toteuttamiseksi WebNavigator on yksinkertaisempi ratkaisu. Etäkäyttöasemia on tarkoitus hankkia vähintään 10, jolloin WinCC WebNavigatoria olisi mahdollista käyttää näistä kaikista etäohjausasemista yhtäaikaisesti. WinCC Sm@rtServeriä voitaisiin käyttää yhtäaikaisesti enintään viidestä etäkäyttöasemasta, mikä ei tule opetuskäytössä riittämään. Myös konsultoitaessa Siemensin edustajien kanssa suositeltiin ratkaisuksi WinCC WebNavigatoria. Kemi-Tornion ammattikorkeakoululla käytössä olevat Windows-käyttöjärjestelmät ovat yhteensopivat Simatic WinCC WebNavigatorin kanssa. Lisäksi WinCC WebNavigator on jo käytössä useissa vedenkäsittelylaitoksissa ympäri maailmaa, joten ohjelmisto soveltuisi senkin puolesta hyvin vesiprosessin ohjaamiseen.

Simatic WinCC WebNavigator on Simatic WinCC RunTime Professionalin sovellus, johon koko etäyhteyden muodostaminen perustuu ja jonka kautta etäohjaaminen tulee tapahtumaan. Pienin lisenssi ei tule riittämään opetuskäytössä, joten Simatic WinCC WebNavigatorista tulee hankkia lisenssi kymmenelle etäohjausasemalle

Etäohjauksen toteuttamiseksi Siemensiltä on hankittava Simatic WinCC Runtime Professional, jonka Simatic WinCC WebNavigator vaatii toimiakseen. Simatic WinCC RunTime Professionalista riittää pienin ja halvin mahdollinen lisenssi. Tässä lisenssissä

PowerTagien eli muuttujien määrä on 128. Lisenssiä on kuitenkin saatavilla aina 64000 muuttujaan asti.

Hankittaessa Simatic WinCC Runtime Professional saadaan myös tulevaisuudessa liitettyä useampia WinCC-sovelluksia verrattuna toisena vaihtoehtona esitetyn Simatic WinCC Sm@rtServerin vaatimaan Simatic WinCC Runtime Advancediin. Näin on myös mahdollisuus korkeampaan ratkaisuiden vakiointiin ilman, että tarvitsee hankkia tulevaisuudessa eri ohjelmistoversioita. Myös tietoturva on korkeampi ratkaisuiden ollessa vakiot. Simatic WinCC Runtime Professionalin hintaan sisältyy myös WinCC Logging sekä Simatic Logon, jotka Advanced-versioon on hankittavissa erikseen.

Tällä hetkellä käytössä on Classic-versiot ohjelmistoista WinCC sekä STEP 7, jotka voivat olla asennettuina ja käytössä tietokoneilla myös hankittavien ohjelmistoversioiden lisäksi. Etäohjauksen toteuttamiseksi Siemensin ratkaisuilla tulee joka tapauksessa päivittää versiot WinCC-työkalusta. Etäohjaus Siemensin WebNavigatorilla on mahdollista toteuttaa joko osana TIA Portalia tai ilman.

Vaihtoehdossa ilman TIA Portalia tarvitaan WinCC-ohjelmistosta versio 7. Tällä hetkellä käytössä olevaa ohjelmistoa WinCC Runtime Flexible ei ole mahdollista päivittää. Hankittaessa ohjelmistoversio Simatic WinCC V7 sisältyy samaan hintaan myös Runtime-ohjelmisto. Lisäksi tulee hankkia luonnollisesti myös WinCC WebNavigator 10 etäkäyttäjän lisenssillä. Vesiprosessin ohjaamiseen riittää pienimmät lisenssit ohjelmistoista WinCC sekä WinCC Runtime.

TIA Portalin kanssa tarvitaan ohjelmistoversio WinCC V11 ES, WinCC Runtime Professional sekä lisäksi WinCC WebNavigator, jossa siis kymmenen etäkäyttäjän lisenssi. Lisäksi käytössä oleviin WinCC Flexible 2008 Advancediin sekä Powerpack WinCC advancediin on hankittava päivitykset. Pienimmät lisenssit ohjelmistoista WinCC sekä Runtime riittävät tässäkin vaihtoehdossa vesiprosessin ohjaukseen. STEP 7 -ohjelmistoa ei ole pakollista päivittää, mutta jos päädytään hankkimaan TIA Portal, niin myös STEP 7 -ohjelmisto olisi järkevä päivittää versioon 11 käytettävyyden kannalta.

Tällä hetkellä Kemi-Tornion ammattikorkeakoululla ei ole käytössä Siemensin tietoturvapalveluita eikä myöskään Siemensin tietoturvaohjelmistoja. Tietoturvan varmistamiseksi Siemensiltä hankitaan rautapalomuuri sekä DMZ-palvelu, joiden avulla Kemi-Tornion ammattikorkeakoululle tuleva WebNavigator-palvelin erotetaan omaksi verkkosegmentikseen. Whitelisting-palvelulla käytössä olevat tietokoneet kovennetaan ainoastaan etäohjausyhteyden käyttöön. Kemi-Tornion ammattikorkeakoululla sijaitseviin, etäyhteyden käyttöön varattuihin tietokoneisiin hankitaan myös Siemensin virustorjuntaohjelmisto. Siemensin WSUS- ja Patch Management -palvelulla suunnitellaan tietoturva, sen päivitykset ja käyttöönotto. Tällä hetkellä käytössä olevat ohjelmistoversiot, hankittavat ohjelmistot, laitteet ja tarvittavat päivitykset ovat liitteessä 1.

6.2. Käyttöönottosuunnitelma

Mikäli WinCC WebNavigator otetaan käyttöön Kemi-Tornion ammattikorkeakoulun tekniikan yksikön automaatiolaboratoriossa, tilataan Siemensiltä valittuun ratkaisuun tarvittavat ohjelmistot, ohjelmistopäivitykset, laitteet sekä palvelut hankintaesityksen mukaisesti joko osana TIA Portalia tai ilman sitä. Kaikki tarvittavat ohjelmistot ja laitteet on oltava asennettuna sekä kaikki tarvittavat toimenpiteet tulee olla suoritettuna ennen etäohjauksen varsinaista käyttöönottoa.

Hankittaessa laitteet ja ohjelmistot selvitetään Siemensin edustajien kanssa toimituksen yhteydessä:

- kaikkien osapuolten vastuut.
- toimintatavat, tiedotus ja tiedonvaihto.
- verkkotopologia ja liityntä verkkoon.
- tietoliikenteen dokumentointi.
- käyttäjätunnukset ja salasanat.
- Kemi-Tornion ammattikorkeakoulun ja automaatiotoimittajan väliset tietoliikenneyhteydet.
- varmuuskopiointi ja tietojen palautus.
- Kemi-Tornion ammattikorkeakoulun muut IT-ratkaisut.

Käyttöönotto tapahtuu asentamalla Siemensiltä tilatut ohjelmistot, ohjelmistopäivitykset, lisenssit sekä tietoturvaohjelmistot käyttöön annettuihin PC-asemiin, jotka sijaitsevat etäkäyttöä varten varatussa tilassa. PC-asemat tulee olla liitettynä Kemi-Tornion ammattikorkeakoulun tekniikan yksikön laboratorion automaatioverkkoon. Myös tietoturvapalvelut tulee olla asennettu ennen varsinaista käyttöönottoa sekä testausta.

Simatic WinCC WebNavigatorin palvelinpohjainen lisenssi asennetaan etäkäyttöä varten varattuihin PC-asemiin. Lisäksi WebNavigatorin etäkäyttölisenssi asennetaan Kemi-Tornion ammattikorkeakoulun sisäverkkoon kuulumattomaan PC-asemaan, jonka avulla myös järjestelmän testaus tulee tapahtumaan. Käytössä olevat S7-300 -logiikat on myös yhdistettävä Profinetin avulla etäyhteyden käyttöön varattuihin PC-asemiin. Profinet-kortit asennetaan logiikoihin ja logiikat yhdistetään PC-asemiin.

Käyttöön otetaan Siemensin virustorjuntaohjelmisto, joka asennetaan etäyhteyden käyttöön varattuihin PC-asemiin. Rautapalomuurit ja DMZ asennetaan etäyhteyden käytössä olevien PC-asemien erottamiseksi omaksi verkkosegmentikseen. Lisäksi etäyhteyden käytössä olevat PC-asemat ja automaatioverkko kovennetaan Siemensin Whitelisting-palvelun avulla. WSUS- ja Patch Management -palvelun avulla Siemensin tietoturvaedustajat luovat suunnitelman tietoturvaratkaisuiden käyttöönottamiseksi. Kaikkien tietoturvaohjelmistojen- ja palveluiden asennukset suoritetaan Siemensin edustajien, IT-Lappian sekä Kemi-Tornion ammattikorkeakoulun automaatiolaboratorion ylläpitohenkilökunnan yhteistyönä tietoturvan ja vesiprosessin toiminnan varmistamiseksi.

Kun kaikki tarvittavat ohjelmistot ja laitteet tietoturvapalveluineen on asennettu asianmukaisesti, testataan järjestelmän toimivuus. Kemi-Tornion ammattikorkeakoulun sisäverkkoon kuulumattomaan etäkäyttöaseman PC-asemaan asennetaan siis etäkäyttölisenssi. Järjestelmän toimivuus testataan yhdistämällä etäkäyttöaseman PC-asema internet-selaimen avulla Kemi-Tornion ammattikorkeakoulun etäkäyttöön varattujen PC-asemien WebNavigator-palvelimeen. Etäyhteys testataan luomalla VPN-yhteys WebNavigator-palvelimen sekä Kemi-Tornion ammattikorkeakoulun sisäverkkoon kuulumattoman PC-aseman välille. Testaus toteutetaan joko luomalla uusi WinCC-projekti, johon luodaan operointinäyttö vesiprosessin ohjaamiseksi tai vastaavasti voidaan

myös käyttää jo mahdollisesti valmiina olevaa, toimivaa WinCC-projektia WinCC-tietokannassa. Käytössä ollevalla WinCC Classic -ohjelmistoversiolla luodut projektit ovat suoraan käännettävissä hankittuun käyttöliittymäversioon.

Järjestelmään luodaan käyttöoikeudet käyttäjäryhmien mukaan Simatic Logonin avulla. Opiskelijoille asetetaan rajatut käyttöoikeudet vesiprosessin ohjaamista ja monitorointia varten sekä järjestelmän ylläpitohenkilöstölle rajattomat käyttöoikeudet. Myös laboratorio-opettajille asetetaan käyttöoikeudet haluttujen ratkaisuiden mukaan.

Järjestelmän ylläpitämiseksi Siemensin edustajien kanssa sovitaan Kemi-Tornion ammattikorkeakoulun, Siemensin sekä IT-Lappian vastuut. Samoin sovitaan toimintatavoista, tiedotuksesta sekä tietoliikenneyhteyksistä. Samoin tietoturvapalveluihin perehdyttämisestä ja koulutuksesta sovitaan Siemensin edustajien kanssa. WinCC-ohjelmistojen ylläpidosta vastaa Kemi-Tornion ammattikorkeakoulun laboratorioiden ylläpitohenkilöstö. Tietoturvan ylläpitämisestä vastaa puolestaan IT-Lappia.

7. ETÄOHJAUKSEN TOTEUTUS ILINC-OHJELMISTON AVULLA

Tällä hetkellä vesiprosessia on mahdollista etäohjata Kemi-Tornion ammattikorkeakoululla MetsoDNA-ohjelmistolla käyttäen apuna iLinc-etäyhteysohjelmistoa. Samaa menetelmää on mahdollisuus käyttää myös etäohjauksen toteuttamisessa Siemensin ratkaisuilla. Kemi-Tornion ammattikorkeakoulun tietoverkko on jaettu kuvan 18 mukaisesti useisiin eri segmenteihin, joita ovat laboratorioverkko, Kemi-Tornion ammattikorkeakoulun sisäverkko sekä DMZ-alue. Lisäksi vielä MetsoDNA-laboratorioverkko on erotettu omaksi verkkosegmentiksi, johon ei pääse käsiksi laboratorioverkon ulkopuolelta. /6/

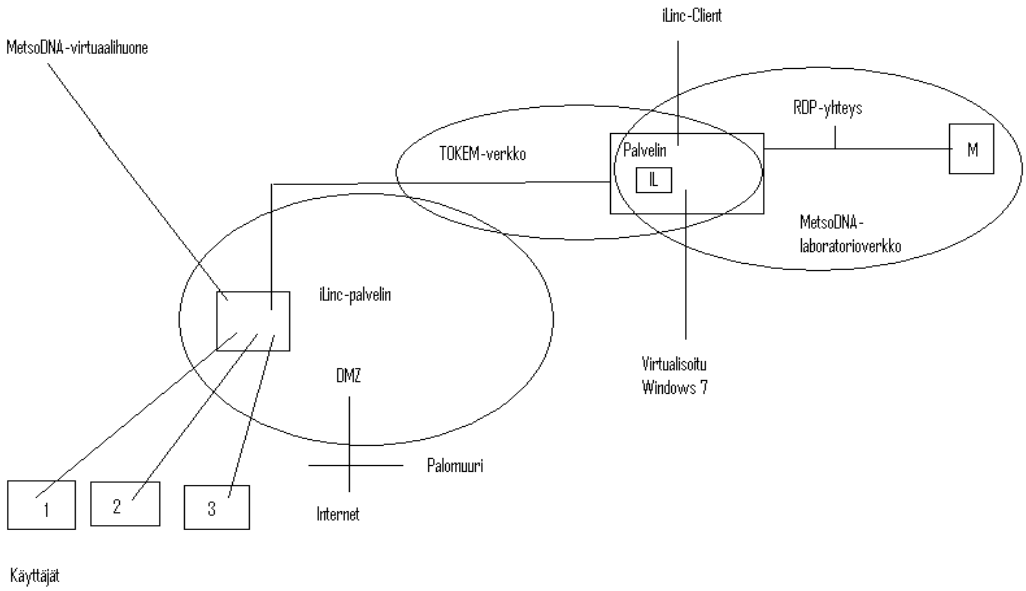
Laboratorioverkossa on PC-asema, jolla voidaan ohjata vesiprosessia MetsoDNA-ohjelmistolla myös paikanpäällä ilman etäyhteyttä. Kemi-Tornion ammattikorkeakoulun sisäverkon ja MetsoDNA-laboratorioverkon välillä on virtualisoitu PC-asema, jossa on käytössä iLinc Client -sovellus. Virtualisoidussa PC-asemassa on 2 eri verkkokorttia, joiden kautta PC-asema on yhdistetty laboratorioverkkoon sekä Kemi-Tornion ammattikorkeakoulun sisäverkkoon. /6/

Virtualisoidussa PC-asemassa on käytössä Windows 7 -käyttöjärjestelmä, jonka kautta on luotu Remote Desktop Protocol -yhteys sisäverkon kautta iLinc-palvelimen ja laboratorioverkossa olevan PC-aseman välille, jonka kautta MetsoDNA-ohjelmistolla siis voidaan ohjata vesiprosessia. Käytännössä ohjaus tapahtuu siten, että Remote Desktop Protocol -yhteyden avulla voidaan hallita etäyhteyden kautta laboratorioverkossa olevan PC-aseman näyttöä ja siten kaikkia kyseiseen PC-asemaan asennettuja ohjelmistoja. Laboratorioverkon PC-aseman näyttö näkyy siis samanlaisena etäkäyttäjän PC-asemassa. /6/

Kemi-Tornion ammattikorkeakoulun sisäverkko on yhdistetty MetsoDNA:n virtuaalihuoneeseen, jossa sijaitsee iLinc-palvelin. Virtuaalihuone sijaitsee DMZ-alueella, joka on erotettu internetistä palomuurin avulla. Kemi-Tornion ammattikorkeakoulun opiskelijat voivat näin yhdistää käyttämänsä PC-aseman iLinc-palvelimeen, josta puolestaan luodaan yhteys virtualisoituun PC-asemaan, jossa on iLinc Client -sovellus.

Virtualisoitu PC-asema tulee kuitenkin olla käytössä, jotta etäyhteyden muodostaminen onnistuu. /6/

Käyttäjät voivat kirjautua opiskelijatunnuksillaan iLinc-palvelimeen. Kun opiskelija on kirjautunut iLinc-ohjelmistoon, vesiprosessia ohjatakseen tulee ottaa puheenjohtajuus, sekä pyytää jakoa MetsoDNA-käyttäjältä. Kun järjestelmään on kerran kirjautunut, hyväksyy iLinc-palvelin jakamisen automaattisesti. Yhtäaikaisesti käyttäjiä voi olla useita. Vesiprosessia voi ohjata kuitenkin vain yksi PC-asema kerrallaan, joten useiden käyttäjien tapauksessa tulee vuorotellen ottaa puheenjohtajuus. Lisäksi on mahdollista ottaa käyttöön video-, ääni-, sekä chat-yhteys ohjelmiston käyttäjien kesken. Lisäksi etäkäyttöasemien sekä iLinc-palvelimen välillä tulee olla riittävästi kaistaa, jottei vesiprosessin ohjauksessa ilmene suurempia viiveaikoja. Viiveaika on normaalisti noin puoli sekuntia./6/



Kuva 18. Vesiprosessin ohjaus iLinc-ohjelmiston avulla

Käytännössä etäohjauksen toteuttaminen Siemensin ratkaisuilla iLincin avulla tulisi tapahtumaan samalla periaatteella kuin esitetyn MetsoDNA-ohjelmiston tapauksessa. iLinc-palvelin yhdistettäisiin virtualisoidun PC-aseman kautta laboratorion

automaatioverkkoon, jossa olisi vesiprosessin ohjaukseen tarkoitettu PC-asema, johon on asennettu Siemensin ohjelmistot etäohjauksen mahdollistamiseksi. Tämän PC-aseman näyttöä voitaisiin sitten hallita iLinc-ohjelmiston kautta myös Kemi-Tornion ammattikorkeakoulun ulkopuolelta.

8. YHTEENVETO

Tässä opinnäytetyössä selvitetään Kemi-Tornion ammattikorkeakoulun tekniikan yksikön automaatiolaboratoriossa käytössä olevan vesiprosessin etäohjausmahdollisuudet Siemensin ratkaisuilla. Etäohjausmahdollisuus olisi hyödyllinen varsinkin aikuisopetuksen kannalta.

Työssä ei ilmennyt suurempia ongelmia. Ongelmia tuotti kuitenkin rajallinen materiaali liittyen Siemensin etäohjausratkaisuihin sekä tietoturva-asiat, joita ei koulutusohjelmassa oltu käsitelty millään tavalla. Tietoa kerättiin, internetistä, kirjalähteistä, Siemensin tuote-esitteistä sekä haastattelemalla Siemensin tuotepäällikköä ja IT-Lappian edustajia sähköpostin välityksellä.

Työn tuloksena on hankintaesitys sekä käyttöönottosuunnitelma sekä toteutusratkaisu iLinc-ohjelmiston avulla. Työn tavoitteet toteutuivat siten, että työssä saatiin selvitettyä Siemensin mahdolliset ratkaisut vesiprosessin etäohjaukseen. Etäohjausta ei kuitenkaan ainakaan toistaiseksi toteuteta valitulla ratkaisulla. Etäohjaus Siemensin ratkaisuilla on kuitenkin mahdollista toteuttaa myös tulevaisuudessa tämän opinnäytetyön pohjalta.

9. LÄHDELUETTELO

/1/ Ahokas, Ilkka, Tuotepäällikon haastattelu, Siemens osakeyhtiö, Espoo 24.1.2012.

/2/ Järvinen, Petteri, Paranna Tietoturvaasi, Docendo, 1. Painos 2006, s 67-69, s 105-120,.

/3/ Kemi-Tornion ammattikorkeakoulu, AMK-esittelysarja 2010, [ppt-dokumentti], [http://www.tokem.fi/Suomeksi/Esittely.iw3] 30.1.2012.

/4/ Kemi-Tornion ammattikorkeakoulu, Automaatiotekniikka, [WWW-dokumentti] [http://www.tokem.fi/?DeptID=15136] 20.2.2012.

/5 / Kemi-Tornion Koulutuskuntayhtymä Lappia, Kemi-Tornionlaakson koulutuskuntayhtymä Lappian langattoman lähiverkon (WLAN) Tietoturvasäännöt, [PDF-dokumentti], [http://www.kkylappia.fi/loader.aspx?id=34782602-0d0d-44ad-b44c-c20bb1caa58c] 3.3.2012.

/6/ Mehtälä, Marko, IT-tukihenkilön haastattelu, IT-Lappia, Kemi, 5.4.2012

/7/ Nikki, Henri Markus, Prosessin käyttöönotto ja viritys Simatic S7- logiikan avulla, Opinnäytetyö, Kemi-Tornion ammattikorkeakoulu 2008, s. 17-21.

/8/ Kontaktia Media Osakeyhtiö, Tietoturva, [WWW-dokumentti], [http://www.internetopas.fi/yleistietoa/tietoturva] 22.11.2011.

/9/ Parviainen, Mika, Poltinohjausten modernisoinnin esiselvitys, Opinnäytetyö, Savonia ammattikorkeakoulu 2011.

/10/ Savolainen, Jani, IT-tukihenkilön haastattelu, IT-Lappia, Kemi 9.3.2012.

/11/ Suomen automaatioseura Ry, Turvallisuusjaosto, Teollisuusautomaation tietoturva, SAS julkaisusarja nro 29, Verkkopainos 2010, s43-45, 65-70.

/12/ Siemens osakeyhtiö, Simatic SEP 7 in the Totally Integrated Portal, [PDF-dokumentti], [http://www.siemens.fi/pool/products/industry/iadt_is/tuotteet/tia_portal/simatic-step-7-in-the-tia-portal.pdf]

/13/ Siemens osakeyhtiö, TIA-Portal-esite (EN), [PDF-dokumentti], [http://www.siemens.fi/fi/industry/teollisuuden_tuotteet_ja_ratkaisut/tuotesivut/tia_portal.php]

/14/ Siemens osakeyhtiö, TIA Portal-esite (FI), [PDF-dokumentti], [http://www.siemens.fi/fi/industry/teollisuuden_tuotteet_ja_ratkaisut/tuotesivut/tia_portal.php]

/15/Siemens osakeyhtiö, WinCC/WebNavigator, [WWW-dokumentti], [http://www.automation.siemens.com/mcms/human-machine-interface/en/visualization-software/scada/wincc-options/wincc-web-navigator/Pages/Default.aspx] 16.2.2012

/16/ Tietokonekauppa.fi, tuotekuvat, [WWW-dokumentti], [http://tietokonekauppa.fi/tuotekuvat/67107_1.jpg] 8.2.2012

/17/ Siemens osakeyhtiö, WinCC/Server, [WWW-dokumentti], [http://www.automation.siemens.com/mcms/human-machine-interface/en/visualization-software/scada/wincc-options/wincc-server/Pages/Default.aspx] 20.2.2012

/18/ Siemens osakeyhtiö, TIA Portal - Teollisuusautomaation ohjelmistoalusta, [WWW-dokumentti],

[http://www.siemens.fi/fi/industry/teollisuuden_tuotteet_ja_ratkaisut/tuotesivut/tia_portal.php] 18.1.2012

/19/ Siemens osakeyhtiö, Siemensin tietoturvapalvelut, [WWW-dokumentti], [http://www.siemens.fi/fi/industry/teollisuuden_tuotteet_ja_ratkaisut/palvelut_ja_koulutus/siemensin_tietoturvapalvelut.htm] 15.2.2012

/20/ Siemens osakeyhtiö, Simatic WinCC flexible/Smartservice, [WWW-dokumentti] [http://www.automation.siemens.com/mcms/human-machine-interface/en/visualization-software/wincc-flexible/wincc-flexible-options/smart-service/Pages/Default.aspx] 1.3.2012

/21/ Siemens osakeyhtiö, SINAMICS Startdrive Commissioning Software, [WWW-dokumentti], [http://www.automation.siemens.com/mcms/mc/en/engineering-software/startdrive/Pages/startdrive.aspx] 12.2.2012

10. LIITELUETTELO

Hankintaesitys

Taulukko 1. Käytössä olevat ohjelmistoversiot:

Ohjelmisto	**Versio**	**Service Pack**
Siemens Simatic WinCC	Advanced Flexible 2008	Kyllä
Siemens Simatic Step 7	5.4	Kyllä
WinCC Runtime	Flexible 2008	Kyllä
Keskusyksiköt (CPU)	314-IFM ja 315-2DP	-

Service-packeihin kuuluu Profinet, joten se toimii myös tietokoneissa, joihin Siemensin ohjelmistot on asennettu. Koululla on logiikoille Profinet-kortteja muutama kappale. Profinet-korteille on paikat S7-300-logiikoiden 315-2DP-malleissa. Siemensin Classic-versiot voivat olla myös yhtä aikaa käytössä TIA Portalin kanssa.

Käytössä oleva tietoturva

- Rautapalomuuri
- Internet-liikenteen suodatus
- Verkkosegmenttien suodatus.
- Virustorjunta (F-Secure)

Hankittavat ohjelmistot:

Taulukko 2. TIA Portalin kanssa

Ohjelmisto	**Versio**	**Tilauskoodi**
Päivitys: Siemens Simatic WinCC Flexible 2008 advanced	WinCC Advanced V11 SP2	6AV2102-4AA01-0AE5
Päivitys: Powerpack WinCC Advanced	Professional 512 PowerTags V11	6AV2103-2AD01-0AC5
WinCC WebNavigator	10 Clients	6AV2107-0KF00-0BB0
WinCC Runtime	Professional 128 PowerTags	6AV2105-0BA01-0AA0
(Siemens Step 7)	Professional Classic + V11 SUS	6ES7810-5CC04-0YE2

Taulukko 3. Ilman TIA Portalia

Ohjelmisto	**Versio**	**Tilauskoodi**
Siemens Simatic WinCC	V 7.0	6AV6381-2BM07-0AX0
WinCC Runtime	Professional 128 PowerTags	6AV2105-0BA01-0AA0
WinCC WebNavigator	10 clients	6AV2107-0KF00-0BB0

Taulukko 4. Siemensin tietoturva

Ohjelmisto/palvelu	Hinta
Palomuuri ja DMZ-palvelu	Tarjouspyyntö
Virustorjunta	Tarjouspyyntö
WSUS- ja Patch Management	Tarjouspyyntö
Whitelisting	Tarjouspyyntö